APPENDIX B

OPEN WIRELESS LAN THEORY OF OPERATION

PREFACE

Purpose of This Book

This book describes the open wireless local area network (LAN) by Norand and the LAN's wireless infrastructure. This book is function-oriented; that is, it describes the network, its components, and how it operates. User guides and other publications for specific open wireless LAN products contain step-by-step design and installation procedures. The end of this section lists related publications.

Intended Audience

The main audience for this book is the system administrator responsible for implementing the site's NORAND® open wireless LAN. This book is intended for sites with established NORAND systems and for sites installing a NORAND system for the first time.

Anyone considering the purchase or installation of the NORAND open wireless LAN will benefit from the information in this book because it describes how the open system provides wireless connectivity solutions. This book will help the network hardware installer because it shows how NORAND open wireless LAN products connect to Ethernet media.

Organization

This book has the following sections and appendixes. The appendixes contain supplemental information about the open system.

Section 1, "Network Terminology"

Section 1 defines some network terms.

Section 2, "The Wireless Infrastructure"

Section 2 provides an overview of the NORAND open wireless LAN's wireless infrastructure by describing how the infrastructure is the mechanism for data transfer between the Ethernet medium and wireless end-user stations.

Section 3, "Wireless Infrastructure Operation"

Section 3 describes how the wireless infrastructure configures itself and operates through its network spanning tree. The section also covers related operations such as frame forwarding, flooding, filtering, and roaming.

Section 4, "Network Configurations"

Section 4 shows examples of network configurations with open wireless LAN network devices.

Section 5, "Network Connectivity"

Wireless network interface cards (NICs) and PEN*KEY® computers by Norand provide a range of network connectivity solutions. Section 5 describes these network products and the solutions they provide.

Section 6, "Host Connectivity"

Section 6 provides an overview of NORAND host connectivity devices and terminal emulation stations. It also describes the terminal emulation protocol stack.

Section 7, "Wireless Access Points"

Section 7 covers wireless access points and the solutions they provide.

Section 8, "Installation"

Section 8 provides useful overviews of design and installation strategies for the open wireless LAN. This section also shows how wireless infrastructure and host connectivity devices connect to Ethernet media.

Section 9, "System Management"

Section 9 covers these system software management tasks: configuring system software through local and remote sessions, downloading the latest version of system software, and querying devices for status information through Simple Network Management Protocol (SNMP).

Appendix A, "Radio Options"

Appendix A describes radio options for the wireless infrastructure and includes radio specifications, international frequencies, and data rates.

Appendix B, "Recommended Network Products"

Appendix B lists network communication products Norand recommends for use with the open system.

Appendix C, "ODI and NDIS Driver Configurations"

Appendix C has examples of Open Data-Link Interface (ODI) and Network Device Interface Specification (NDIS) driver configurations for the PEN*KEY 6100 Computer.

Appendix D, "6710 Access Point Specifications"

Appendix D covers electrical, mechanical, and physical specifications for the NORAND 6710 Access Point.

Appendix E, "Host Connectivity Device Specifications"

Appendix E covers electrical, mechanical, and physical specifications for the NORAND RC4030E Gateway and 6950 Enterprise Gateway Server.

Related NORAND Publications

For more information about specific NORAND open wireless LAN products, refer to the following publications. Numbers in parentheses indicate the Norand part number (NPN) of the publication.

▶ NOTE: *We welcome your comments about this Open Wireless LAN Theory of Operation and our other publications. Please write your comments on the Reader's Comments card included with the publication and then drop the card in the mail.*

Access Point User Guide

6710 Access Point User's Guide (NPN: 961-047-081)

The user guide for the 6710 Access Point describes how to install, configure, and troubleshoot the access point.

PEN*KEY Computer User Guides

PEN*KEY computer user guides describe how to set up, operate, and maintain PEN*KEY computers. Specific user guides are:

*PEN*KEY 6100 Computer User's Guide (NPN: 961-028-085)*

*PEN*KEY 6400 Computer User's Guide (NPN: 961-028-093)*

*PEN*KEY 6600 Computer User's Guide (NPN: 961-028-084)*

PEN*KEY Computer Programmer Guides

PEN*KEY computer programmer guides contain information about windows applications, power management, system and device support, and system messages for PEN*KEY computers. Programmer guides also cover tool kits. Specific programmer guides are:

*PEN*KEY Model 6100 Computer Programmer's Reference Guide (NPN: 977-054-001)*

*PEN*KEY Model 6200/6300 Computer Programmer's Reference Guide (NPN: 977-054-003)*

*PEN*KEY Model 6600 Computer Programmer's Reference Guide (NPN: 977-054-002)*

Host Connectivity Device User Guides

6910 Integrated Gateway/Access Point User's Guide (NPN: 961-047-095)

The 6910 Integrated Gateway/Access Point combines the host functionality of the RC4030E Gateway and access point functionality of the 6710 Access Point. The user guide describes how to install, configure, and troubleshoot the gateway/access point.

6950 Enterprise Gateway Server User's Guide (NPN: 961-047-091)

The user guide for the 6950 Enterprise Gateway Server describes how to install and configure the gateway server.

RC4030E Gateway User's Guide (NPN: 961-047-087)

The user guide for the RC4030E Gateway describes how to install, configure, and troubleshoot the gateway.

Wireless Network Access Server User's Guide (NPN: 961-051-006)

This user guide describes how to configure the Wireless Network Access Server software, which runs on a host platform.

Terminal Emulation Station User Guides

Terminal emulation station user guides describe how to set up, operate, and maintain radio terminals in each series of terminal. Specific user guides are:

1100 Series User's Guide (NPN: 961-047-069)

*PEN*KEY 6400 User's Guide (NPN: 961-028-093)*

RT1700 Radio Terminal User's Guide (NPN: 961-047-068)

RT5980 Radio Terminal User's Guide (NPN: 961-047-092)

Development Kit Manuals

▶ NOTE: *See also PEN*KEY Computer Programmer Guides.*

Application Developer's Kit Reference Manual Volume A (NPN: 977-051-004) and Volume B (NPN: 977-051-005)

These two volumes cover the commands programmers can use to write various applications for NORAND terminal emulation stations.

Terminal Emulation Programmer Guides

3270 Terminal Emulation Programmer's Reference Guide (NPN: 977-047-040)

This guide describes how terminal emulation stations emulate IBM 3278 Model 2 terminal operation through the 3270 data stream. This guide also covers asynchronous controller commands, and terminal emulation station commands and orders.

5250 Terminal Emulation Programmer's Reference Guide (NPN: 977-047-039)

This guide describes how terminal emulation stations emulate IBM 5291 Display Station operation through the 5250 data stream. This guide also covers 5250 display data stream commands.

Native Terminal Emulation Asynchronous Programmer's Reference Guide (NPN: 977-047-038)

This guide describes components in the radio network using asynchronous NORAND Native communications. This guide also contains commands and orders terminal emulation stations can accept from a host.

VT220/ANSI Terminal Emulation Programmer's Reference Guide (NPN: 977-047-037)

This guide describes how terminal emulation stations emulate VT220 terminal operation. This guide also describes VT220 received codes, transmitted codes, and character sets.

System Management Publications

NORAND Management Information Base Reference Manual (NPN: 977-051-002)

This manual describes the private NORAND Management Information Base (MIB) for the 6710 Access Point, RC4030E Gateway, and 6910 Integrated Gateway/Access Point.

NORAND Open Wireless LAN with HP OpenView for Windows User's Guide (NPN: 961-051-009)

This guide describes how to install and use the OpenView for Windows network management platform by Hewlett-Packard (HP).

OWLView for HP OpenView for Windows User's Guide (NPN: 961-051-010)

This guide describes how to install and use the OWLView for HP OpenView for Windows network management platform.

Related Standards

Related standards include ANSI/IEEE standards and Request For Comments (RFC) documents.

ANSI/IEEE Std 802.3 (ISO/IEC 8802-3)

The Local and Metropolitan Area Network standard specifies the media access control characteristics for the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method. The standard also specifies the media, Medium Attachment Unit (MAU), and physical layer repeater unit for 10 MB/s baseband and broadband systems. Specifications for 10BASE2, 10BASE5, and 10BASE-T are included.

ANSI/IEEE Std 802.11 [DRAFT]

This draft standard specifies the rules of interoperability for wireless network components. The 802.11 standard was still in development when this book was printed. The standard is scheduled for completion in 1996 and submission to ANSI in 1997.

RFC1155

RFC1155 provides the common definitions for the structure and identification of management information for Transmission Control Protocol/Internet Protocol–based (TCP/IP) internets.

RFC1157

RFC1157 defines a simple protocol (SNMP) by which management information for a network element may be inspected or altered by logically remote users.

RFC1213

RFC1213 describes the management information base (MIB) for network management of TCP/IP–based internets (MIB-II).

Customer Support

The goal of Norand Corporation is 100 percent customer satisfaction. If you need assistance with the open wireless LAN, contact Norand through the Customer Response Center.

In the United States, call:	800-221-9236 *or* 319-369-3533
In Canada, call:	800-633-6149
FAX:	319-369-3453
	(ATTN: Customer Response Center)
Mailing address:	Norand Corporation
	ATTN: Customer Response Center
	550 Second Street SE
	Cedar Rapids, IA 52401

Section 1

Network Terminology

Access Point

Access points provide the following functions:

- A *wired bridge* is an access point that attaches to the network through an Ethernet link and has bridging enabled (through access point configuration menus). A wired bridge converts wireless LAN frames to Ethernet frames, and Ethernet frames to wireless LAN frames. A wired bridge also forwards wireless LAN frames to wireless LAN nodes.
- A *designated bridge* is an access point that bridges frames to and from a secondary Ethernet LAN or secondary Proxim LAN. A designated bridge for a secondary Ethernet LAN attaches to the network through a radio port.
- A *wired access point* is an access point that attaches to the network through an Ethernet link and has bridging disabled (through access point configuration menus).
- A *wireless access point* is an access point that attaches to the network through a radio port. A wireless access point provides a wireless store-and-forward operation with frames transmitted over the wireless media to reach their destination. Note that a wireless access point forwards frames; a *wired bridge* forwards *and* bridges frames.

NOTE: *Section 3, "Wireless Infrastructure Operation," contains detailed examples of each type of access point.*

Backbone

A *backbone* is a main cable running vertically or horizontally in a building to provide wired connectivity to different areas in the building. Lower tiers of subnetworks attach to the backbone through bridges, routers, or other internetwork devices. A backbone is not designed for direct system access. Examples of backbone media include Fiber Distributed Data Interface (FDDI) and Token Ring.

Bridging

In this document, *bridging* refers to the translational bridging process of converting open wireless LAN frames to Ethernet frames, and Ethernet frames to open wireless LAN frames.

Direct Sequence

Direct sequence is a spread spectrum technique by which the transmitted signal is spread over a wide frequency range. In a direct sequence system, the bandwidth is large relative to the data rate.

Distribution LAN

The *distribution LAN* is the Ethernet segment to which the access point super root connects. Distribution LAN is also called *primary LAN*.

Ethernet

In this book, *Ethernet* is a general term indicating both 802.3 and DIX Ethernet (also called Ethernet 2.0).

Forwarding

A frame is forwarded by sending it to the next hop on the path to the final destination. All access points (including wireless access points) forward frames.

Frequency Hopping

Frequency hopping is a spread spectrum technique by which the band is divided into a number of channels and the transmissions hop from channel to channel is in a specified sequence.

Infrastructure

The *infrastructure* is the permanently-installed elements of the open wireless LAN. It provides coverage and connectivity between wireless devices throughout the service area.

LAN (Local Area Network)

A *LAN* is a group of network devices in which each device can communicate through a wired or wireless link. The wired link may be composed of several segments joined by repeaters and bridges. The LAN is characterized by the relatively short distance it is designed to cover, a high speed of operation, and relatively low error rates. The geographic scope of LANs is limited to thousands of feet or closely-spaced building complexes.

Media Access Control (MAC) Sublayer

The *MAC sublayer* is the lower portion of the Data Link layer of the Open Systems Interconnection (OSI) model. Norand has divided the MAC sublayer into MACR and MACD.

Open System

An *open system* comprises protocols and components that meet standards set by industry-accepted governing bodies. The standards ensure that when new protocols and components are introduced into an existing system, the protocols and components will meet the standards and be able to communicate with the existing system. The OSI model is the basis for a system to communicate with any other system. The model is a framework of standards Norand uses to create protocol stacks and applications for their network products.

Primary LAN

The *primary LAN* is the Ethernet segment to which the access point super root connects. Primary LAN is also called *distribution LAN*.

Radio Network

The *radio network* consists of radio-enabled network devices and communication paths. It is a group of fixed-end devices and wireless stations in which each can communicate with at least one other device through either a radio or wired Ethernet link. Secondary Ethernet LANs are part of the radio network; the distribution LAN is not part of the radio network.

Secondary Ethernet LAN

A *secondary Ethernet LAN* is an Ethernet segment that connects to the distribution LAN through a wireless link. A single access point functions as the *designated bridge* for the secondary LAN.

Secondary Proxim LAN

The radio coverage area of the Proxim 2.4 GHz radio option is a *secondary Proxim LAN*. The designated bridge for the secondary Proxim LAN is the access point with the radio.

Segment

In LANs, a *segment* is a length of cable from termination to termination. For example, a 10BASE2 cable segment is the length of cable between the 50-Ohm terminators that attach to each end of the cable. For proper network communications, cable segments must meet ANSI/IEEE standard specifications.

Subnet

A *subnet* is a subset of a network that shares a network address with other subnets but is distinguished by a unique subnet number.

Super Root

The *super root* is a wired bridge that operates as the central control point for network-wide parameters, network registration, and other operations. The super root connects to the distribution LAN through an Ethernet link, and is the root node in the open wireless LAN spanning tree.

Terminal Emulation

Terminal emulation enables a wireless station to communicate with a host system that is set up to communicate only with a specific type of terminal (such as used for the 3270 and 5250 data streams). Terminal emulation causes the terminal emulation station to operate almost exactly as the type of terminal the host is programmed to expect.

Terminal Emulation Stations

Terminal emulation stations are PEN*KEY® 6400 Computers and radio terminals set up for 3270, 5250, NORAND® Native, or VT220 terminal emulation. Radio terminals include models in the RT1100, RT1700, and RT5900 Series.

Wireless Network Interface Card (NIC)

A *wireless NIC* is a connectivity device with an internal antenna or with an attached antenna unit.

Wireless Stations

Wireless stations is an inclusive term that refers to the following:

- PC-compatible computing stations equipped with Type III, Type II, mini-ISA, or ISA NICs. PC-compatible computers are PEN*KEY 6100, 6400, and 6600 Computers by Norand, and third-party laptop, notebook, and desktop computers.
- NORAND terminal emulation stations equipped with internal radios or field-replaceable radio modules. Terminal emulation stations are PEN*KEY 6400 Computers and radio terminal models in the RT1100, RT1700, and RT5900 Series.

Section 2

The Wireless Infrastructure

About This Section

The open wireless LAN is a general purpose wireless infrastructure that conforms to the OSI model. This section provides an overview of the wireless infrastructure, its main components, and data flow through its protocol stack.

What is the Wireless Infrastructure?

The wireless infrastructure provides data transfer between the wired physical medium and wireless computing stations, and may provide a wireless link between wired Ethernet segments. Because the infrastructure operates at the MAC sublayer of the OSI Data Link layer, the infrastructure is transparent to most industry-standard communication protocols, and supports arbitrary protocol stacks above the MAC sublayer. The result is wireless connectivity support for applications such as transaction-oriented client-server computing and file transfers.

In addition to providing wireless connectivity to computing stations, the wireless infrastructure supports portable operation within the wireless environment. This support includes power conservation for battery-operated devices and seamless roaming of wireless stations between access point coverage areas.

Benefits

Following is a summary of wireless infrastructure benefits.

Best-path frame forwarding

Media (radio) independence

MAC-layer bridging

Protocol independence

Management through SNMP

Management through RS-232 serial diagnostic port or remote TELNET session to view and change the system configuration

Electronic software distribution through Trivial File Transport Protocol (TFTP) over the network backbone

Security

Automatic or manual network configuration (redundancy) through a spanning tree

Power management for battery operated stations

Unicast and multicast flooding and filtering options

Roaming

Wireless access points

Wireless point-to-point and multidrop bridging

Service for NORAND® gateways and terminal emulation stations

Direct connection to 10BASE2, 10BASE5, or 10BASE-T Ethernet

Components

The wireless infrastructure consists of access points wired to a physical medium (in most cases Ethernet), wireless access points (optional), and a family of wireless NICs that conform to PC card and ISA bus standards.

Wireless NICs install into these PC-compatible computing stations:

- Portable, hand-held PEN*KEY® computers by Norand.
- Third-party computers equipped with a PC card slot or ISA bus slot. Computers equipped with these slots include portable notebooks and laptops, and desktop stations.

Section 5, "Network Connectivity," describes the NICs and PC-compatible computers for the open wireless LAN.

Norand also offers high-performance network gateways and terminal emulation stations, which interconnect with VT220, 5250, 3270, and NORAND Native host applications. Emulation products use the services of the wireless infrastructure, which lets multiple terminal emulation applications and standard applications share a common infrastructure. Section 6, "Host Connectivity," describes host connectivity solutions, NORAND terminal emulation stations, and the terminal emulation protocol stack.

Integrated support for wireless communications is a feature of many wireless computing stations. Integration provides improved ruggedness and low profile antennas. These products provide the same open systems device driver support as the general purpose wireless NICs.

Ethernet Physical Medium

You can install a separate segment of the Ethernet physical medium for the open wireless LAN to specifically support the installation. Or, you can connect access points to the site's existing Ethernet medium to provide a transparent extension to an enterprise network. Section 8, "Installation," shows how NORAND access points and gateways connect to 10BASE2, 10BASE-T, and 10BASE5 Ethernet media.

The wired LAN can comprise several cable segments joined by repeaters and off-the-shelf transparent bridges. Usually, the LAN is in one building or several buildings near each other at the same site. Section 4, "Network Configurations," shows examples of network configurations with LANs in the same building, and in separate buildings connected by a wireless link. Section 8 contains general information about Ethernet segments, repeaters, and off-the-shelf bridges.

Multiple Ethernet LANs can connect to the enterprise network through routers. Section 8 contains general information about routers.

Access Point

The access point is the core of the wireless infrastructure. Figure 2-1 shows current designs of the NORAND 6710 Access Point. Information in this book applies to both designs.

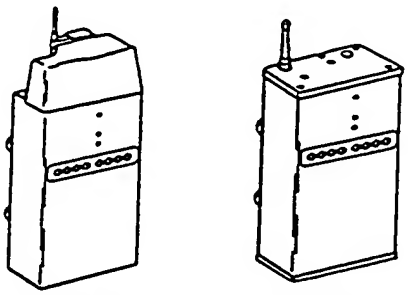


Figure 2-1
6710 Access Points

The access point operates as a protocol-independent bridge by providing transparent, wireless communications for the enterprise LAN. In general, the access point forwards frames from any network node to any other network node on the path through the access point. For example, the access point does the following:

- Forwards frames generated by a wireless station and destined for a host or server on the wired LAN.
- Forwards frames appearing on the wired LAN and destined for a wireless station within the access point's coverage area.
- Forwards frames generated by a wireless station and destined for another wireless station within the same basic service area.
- Forwards frames between wired Ethernet segments across a radio link or links.

Media Independence

The access point accepts a variety of field-replaceable, modular radios through two Type II or Type III PC card-compatible slots for the installation of wireless NICs (Figure 2-2).

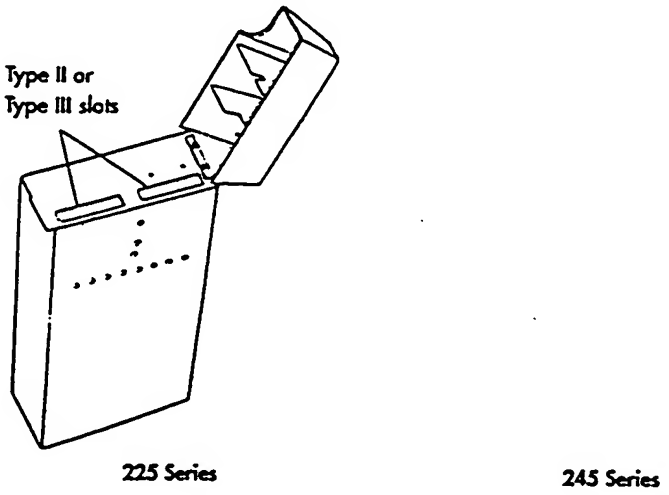


Figure 2-2
Wireless NIC Slots

The NICs enable you to adapt the system to provide different data throughput and coverage tradeoffs depending on required usage. See Appendix A, "Radio Options," for wireless NIC options and specifications.

▶ NOTE: *The access point does not support arbitrary PC cards. Specific PC card software drivers are required.*

Media independence allows you to replace a wireless NIC. Because you can separate the radio from the access point, you do not need to replace the entire installed wireless infrastructure if your network requirements change. You can either upgrade an existing solution or add additional functionality.

Media independence lets you take full advantage of your wireless investment by providing a cost-effective migration path to future wireless networking technologies. Media independence also provides flexibility to support new technology and emerging industry standards (such as 802.11) or alternative defacto standards.

System software loaded in the access point detects the type of radio option installed in the NIC slot. When you configure the access point, the software automatically displays the parameters that match the radio option. If you install a different radio option in the slot, you do not need to load radio-specific system software into the access point.

Radio Operation

900 MHz and synthesized UHF radio options are manufactured by Norand. The 900 MHz radio can operate in the United States, Canada, Australia, and South American countries that allow 900 MHz operations.

The UHF radio can operate in licensed or unlicensed frequency bands throughout the world, subject to national regulations. See Appendix A for country-specific frequencies and data rates.

The 2.4 GHz radio option is a member of the RangeLAN2 family of wireless NICs by Proxim, Inc. The Proxim 2.4 GHz radio can operate in areas that allow use of spread spectrum wireless communications at 2.4 GHz, including Australia and countries in North and South America, Europe, and Asia. In many countries operation without a site license is permitted. Consult a Norand Sales Representative, your local distributor, or a national regulatory agency for details.

Access Point Protocol Stack

The access point operates at the MAC sublayer of the Data Link layer of the OSI protocol model. The MAC sublayer provides services to the Logical Link Control (LLC) sublayer of the Data Link layer. By operating at the MAC sublayer, the access point operates transparently to protocols above the MAC sublayer.

Basic Bridge Operation

A bridge is a device that interconnects LANs. Bridges receive frames sent on each attached network and selectively forward frames between LANs, and use Data Link layer addresses to determine whether to forward each frame. Because bridges operate at the Data Link layer they are not required to examine information from the upper layers, which means they can forward traffic from any network layer protocol.

OSI Model and Access Point Protocol Stack

Figure 2-3 shows the OSI model and access point protocol stack.

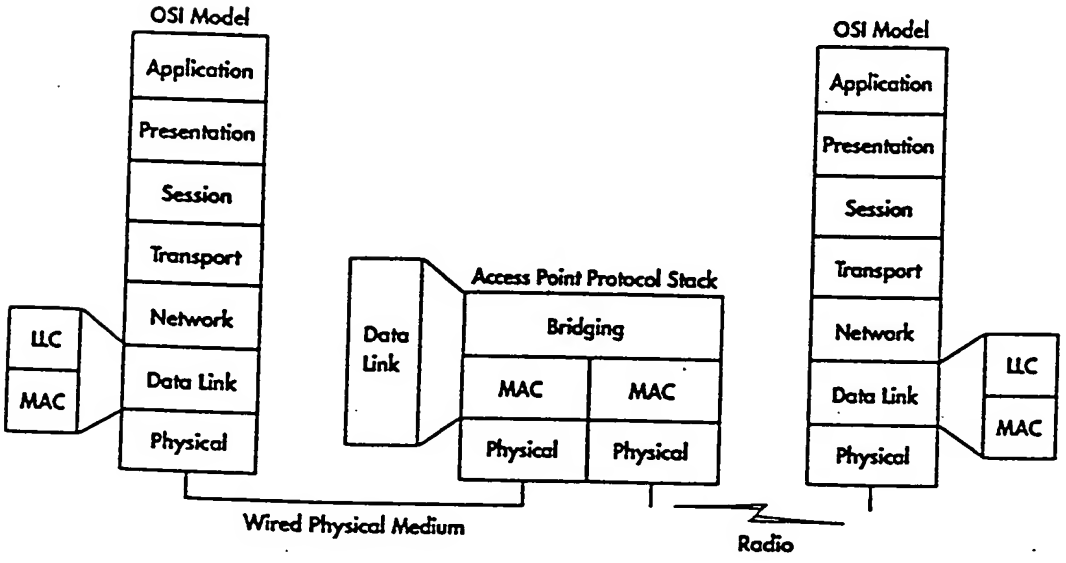


Figure 2-3
OSI Model and Access Point Protocol Stack

Norand divides the MAC sublayer into two functional layers called MACD and MACR.

- MACD is the link protocol, and is responsible for channel access and error free transmission of frames between wireless stations or access points (or both). MACD is media specific and is optimized for the underlying physical medium (wireless radio or wired Ethernet).
- MACR is media independent. It provides facilities for coordination of the infrastructure, roaming of wireless stations between access point coverage areas, and power management to extend the battery life of portable stations.

Figure 2-4 shows the access point protocol stack and communication protocol stacks above the MAC sublayer. The protocol stack above the Bridging layer provides access point management and configuration.

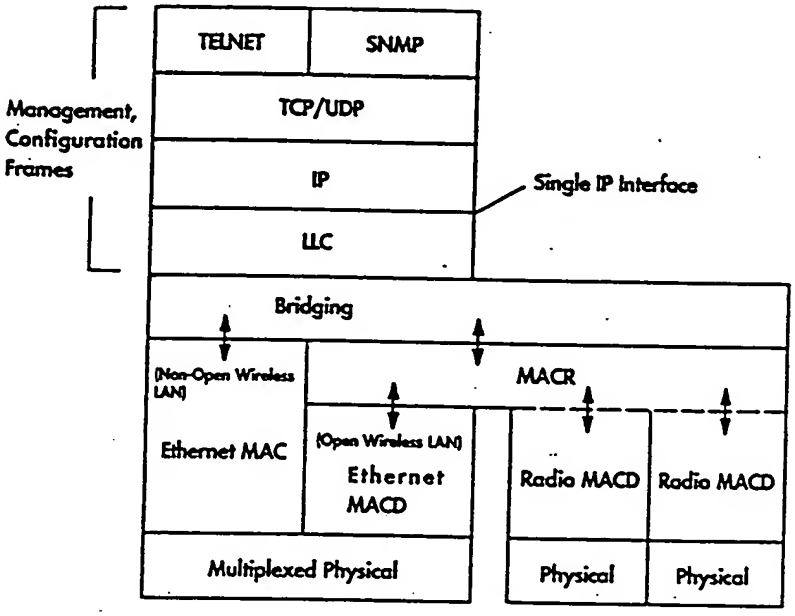


Figure 2-4
Access Point Protocol Stack

Data Flow

Figure 2-5 shows data flow through the access point protocol stack for stations with the 900 MHz, UHF, or Proxim 2.4 GHz radio option.

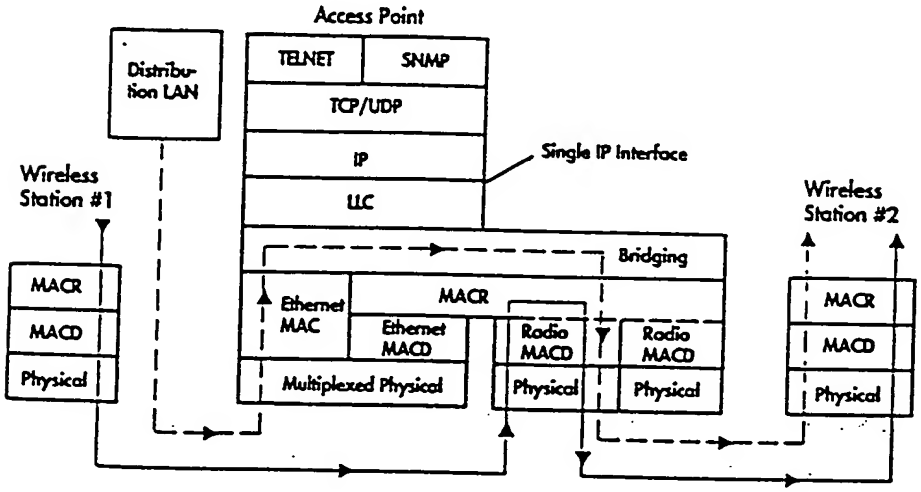


Figure 2-5
Data Flow Through Access Point Protocol Stack

Dashed lines in Figure 2-5 represent the path a frame takes as it travels from a wired station on an Ethernet LAN to a wireless station. The access point *bridges* the frame from the Ethernet LAN to the radio network. (In this document, *bridging* is the translational bridging process of converting open wireless LAN frames to Ethernet frames, and Ethernet frames to open wireless LAN frames.)

Solid lines in Figure 2-5 represent the path a frame takes as it travels from wireless station #1 in the radio network to wireless station #2. Because the path is within the radio network, the access point does not bridge the frame.

Protocols

The wireless infrastructure supports a range of industry-standard communication, management, and configuration protocols, including TCP/IP, NetWare (IPX/SPX), DECnet, and NetBIOS. You can use the standard protocols to transport information from clients (nodes) on the network. This capability does not require knowledge of proprietary tools, application program interfaces, and libraries.

Communication Protocols

The access point is protocol-independent. It uses MAC sublayer addresses to bridge or forward (or bridge *and* forward) frames between stations.

Management and Configuration Protocols

The wireless infrastructure provides management and configuration through a command interpreter and SNMP. You can access the command interpreter through a remote TCP/IP TELNET session or locally through the access point's RS-232 serial diagnostic port for out-of-band management.

SNMP is the most common industry-standard protocol for managing devices on an IP-based network. The resident SNMP agent for NORAND access points and gateways complies with MIB-II standards for information exchange in TCP/IP environments. SNMP-based commands from remote sites are also possible.

TCP/IP is the suite of transport and application protocols that run over IP. The access point and gateway contain an embedded TCP/IP stack. After you assign IP and subnet mask addresses to an access point or a gateway through its configuration menus, you can configure it through a local or remote TELNET session.

You can also update the access point with the latest version of system software through TFTP over the network backbone. Section 9, "System Management," provides more information about TFTP, TELNET, and SNMP.

Section 3

Wireless Infrastructure Operation

About This Section

This section describes how the wireless infrastructure configures itself and operates through a spanning tree. This section also covers related operations including frame forwarding, flooding, filtering, and roaming.

The open wireless LAN by Norand provides extensive system capabilities to resolve unique issues with wireless communications. Because of operational differences among radio options, not all features will provide all of the capabilities discussed in this section. Differences are discussed in the appropriate paragraphs in this section. The open wireless LAN architecture is flexible, allowing new capabilities to be introduced as new wireless media become available.

Wireless Communication Issues

The open wireless LAN resolves a range of unique issues associated with wireless communications, including the following:

- Installation issues and wiring costs
- Radio technology tradeoffs and evolution
- Portable, battery operated wireless stations
- Wired and wireless stations coexisting on the same backbone
- Dynamic radio coverage

Installation Issues and Wiring Costs

A separate segment of the Ethernet physical medium can be installed to specifically support the open wireless LAN installation. Access points and NORAND® gateways can also connect to the site's existing Ethernet medium to provide a transparent extension to an enterprise network.

Access points and gateways are designed to physically connect to 10BASE-T, 10BASE2, and 10BASE5 Ethernet. An access point with the 900 MHz or UHF radio option can operate as a wireless access point, which does not require connection to the Ethernet medium.

Radio Technology Tradeoffs and Evolution

A major issue in radio technology decisions involves range versus speed tradeoffs, with faster radios having reduced communication range. Higher speed radios increase system costs because a 50 percent reduction in the range of a radio results in a need for about four times the number of access points to cover the same area.

Depending on required usage, wireless NICs in the access point enable the system to be adapted to provide different data throughput and coverage tradeoffs. Because the radio separates from the access point, the entire installed wireless infrastructure does not need to be replaced if network requirements change. For example, the following approaches can be employed to meet changing network requirements:

- An additional radio can plug into the access point's second PC card slot to provide a second data channel.
- If new radio technology evolves (such as 802.11), the new radio can plug into the second slot to support incremental growth on the network and also support the existing population on the initial radio.
- If complete migration to new technology is required, only the radio needs to be changed.

In each approach the initial investment in the infrastructure remains intact and the interface to the enterprise network stays the same.

Portable, Battery-Operated Wireless Stations

Because the radio range of a single access point is limited, multiple access points provide coverage over a large area. The access points are installed to provide adjacent areas of coverage, ensuring that as a wireless station moves out of the range of one access point, it roams into the range of another. Figure 3-1 shows a wireless station roaming from coverage area B to A.

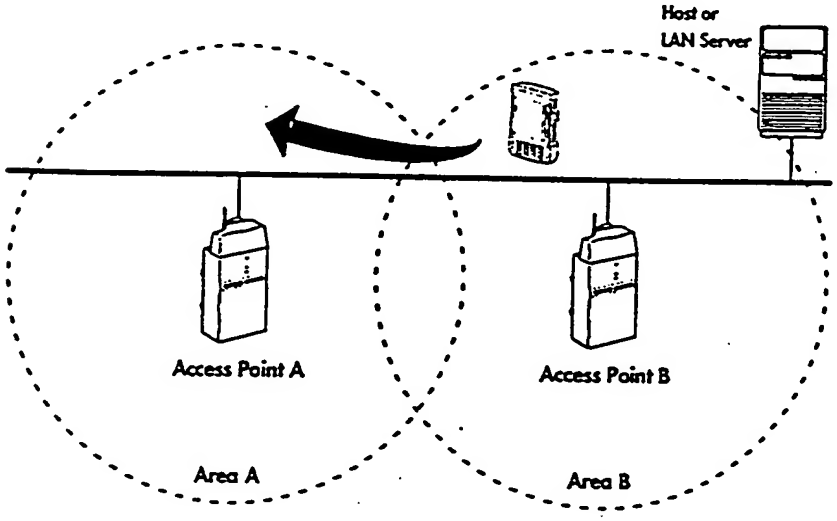


Figure 3-1
Roaming

Areas A and B overlap coverage. When the wireless station leaves the transmission range of access point B, it roams from B to A.

The link with the wireless station is transparently handed from access point to access point without affecting the wireless station's connection to the enterprise LAN. Roaming challenges traditional network design assumptions for the following reasons:

- A roaming wireless station's network address is no longer equal to its physical location.
- Battery-powered mobile computers typically do not maintain continuous connections with the network because advanced power management techniques cycle the radio off when not actively communicating.

Wireless networking software, embedded in the access points, addresses both issues. The access points track the location and status of wireless stations through spanning tree forwarding databases, and manage traffic accordingly. This capability isolates the LAN environment from the issues of mobile devices and transparently integrates the access point based infrastructure into the enterprise network.

Wired and Wireless Stations on Same Backbone

Wired and wireless stations can coexist on the same backbone. An access point operating as a wired bridge provides connectivity to the wireless stations by bridging radio traffic from these devices onto the wired enterprise LAN. The wired bridge converts open wireless LAN frames to Ethernet frames, and Ethernet frames to open wireless LAN frames.

Unicast or multicast flooding options (or both) can be configured for Ethernet LANs through the access point's configuration menus. Programmable and DIX Ethernet filtering options can also be defined to selectively discard Ethernet frames the access point receives on its Ethernet port.

EXAMPLE: In the sample configuration in Figure 3-2, the PEN*KEY® computer and notebook can communicate with the fixed desktop station. To the host and server, the wireless stations appear to be hard-wired to the LAN.

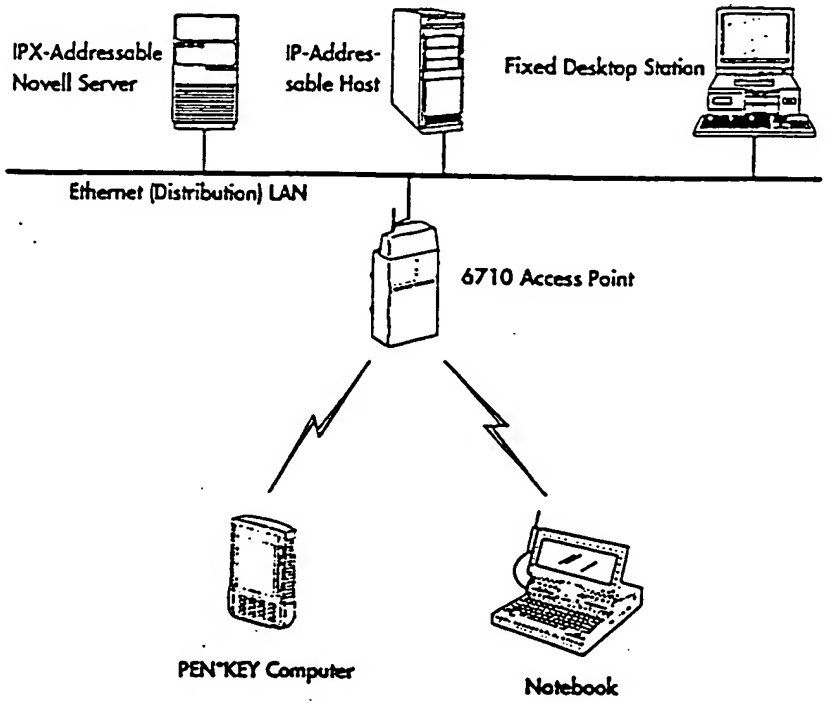


Figure 3-2
Wired and Wireless Stations on Same Backbone

Dynamic Radio Coverage

When access points are powered on, they begin communicating with each other to facilitate the best communications from a wireless station to a server or host. The wireless access point community sets up a hierarchy called a spanning tree, a distributed data structure that optimizes forwarding of messages to wireless stations.

The open wireless LAN spanning tree dynamically organizes the network into a loop-free structure for efficient forwarding of messages. For connectivity, there must be at least one physical path (Ethernet or radio) to each node. If there are multiple possible paths between nodes, the network autoconfigures so that the most efficient link is used. If a link is lost the network dynamically reconfigures to provide an alternative path.

Figure 3-3 shows the physical links in a sample network configuration.

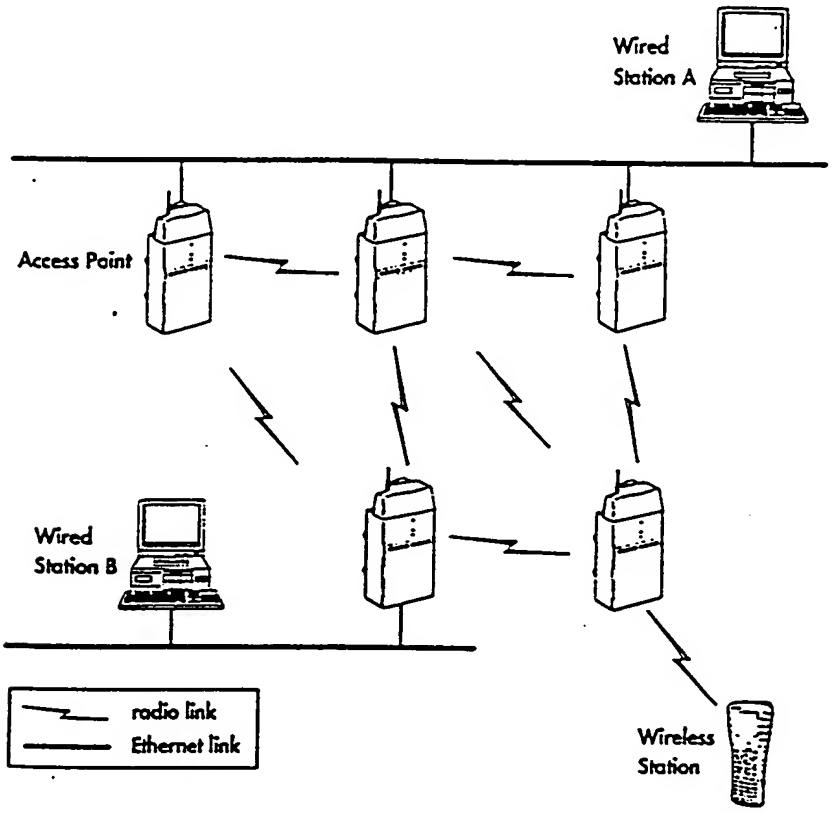


Figure 3-3
Physical Links in Sample Network Configuration

In Figure 3-3, wired station A is not part of the network spanning tree. Wired station B and the Ethernet link it is on can be viewed as part of the spanning tree.

A branch in the spanning tree is a logical link; open wireless LAN frames are forwarded along the branches. Figure 3-4 shows the network in Figure 3-3 organized as a logical network spanning tree. Note that the spanning tree eliminates the loops in the physical topology and uses the most efficient link.

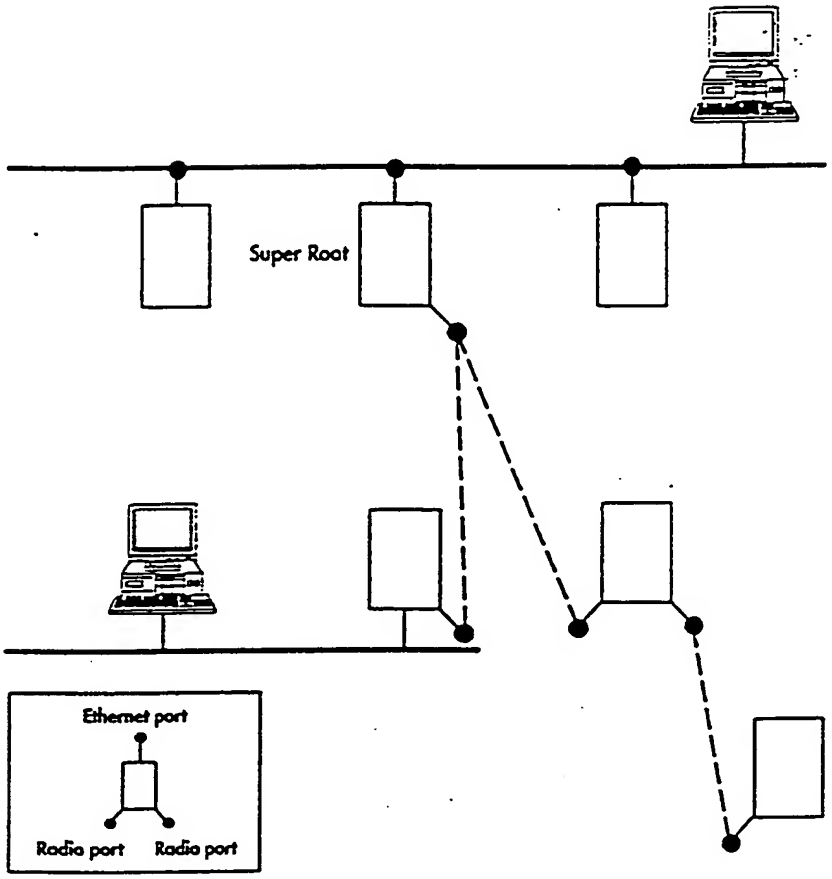


Figure 3-4
Logical Network Spanning Tree

The spanning tree is organized automatically among the nodes of the wireless community. Bridges that are 802.1d compliant also employ a spanning tree architecture. The open wireless LAN spanning tree is designed to overlay 802.1d spanning trees to provide correct operation of wireless nodes in a bridging environment.

Spanning Tree

The open wireless LAN spanning tree can consist of these nodes:

- Multiple access points operating as *wired bridges* and *wireless access points* along the branches of the tree.
- One wired bridge operating as the *super root* of the tree.
- One access point operating as the *designated bridge* for each secondary Ethernet LAN.
- *Wired stations* and *wireless stations* as leaves on the tree.

Figure 3-5 shows a sample network configuration with spanning tree nodes.

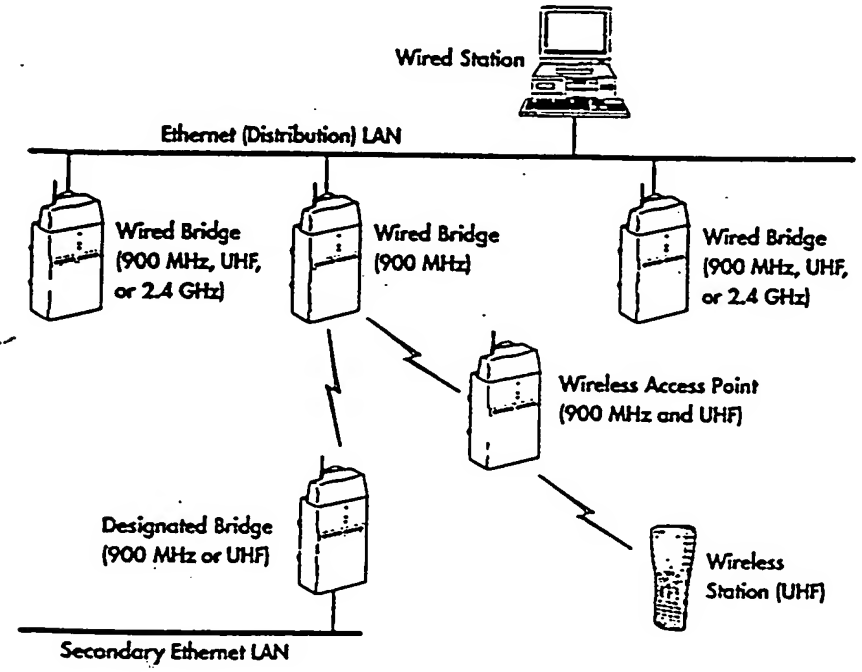


Figure 3-5
Sample Network Configuration

An open wireless LAN node logically attaches to its *parent* through the node's *root port.*

▶ NOTE: *Open wireless LAN nodes are NORAND access points and any wireless station that connects to the network through a NORAND 900 MHz or UHF radio.*

In Figure 3-5 the root port for the wired bridges is the *Ethernet port.* The root port for the wireless access point, designated bridge, and wireless station is the *radio port.* Figure 3-4 on page 3-7 illustrates the port concept.

Wired Bridges

A *wired bridge* is an access point that converts (bridges) an open wireless LAN frame to an Ethernet frame, and an Ethernet frame to an open wireless LAN frame. The wired bridge also forwards open wireless LAN frames to open wireless LAN nodes.

Wireless Access Points

An access point that does not physically connect to the Ethernet medium is a *wireless access point.* It forwards frames through its parent or another wireless access point, or through an access point on the distribution LAN. The parent is the access point to which the wireless access point logically attaches.

▶ NOTE: *The distribution LAN is the physical segment to which the super root physically connects. Usually, the distribution LAN is also the segment to which the primary Ethernet host, LAN server, or NORAND gateway connects.*

Super Root

The open wireless LAN spanning tree must have a root, which is the *super root.* Similarly, each access point is the root of the subtree below the access point. The super root is a wired bridge that operates as the central control point for network-wide parameters, network registration, and other operations.

Super Root Selection

If a network has one super root candidate, that candidate becomes the super root on the distribution LAN.

If a network has two or more super root candidates, the candidate with the highest *root priority* automatically becomes the super root. The range of root priorities is "0" (zero) through "7," where "7" is the highest priority. An access point with priority "0" cannot become a super root.

If two or more access points have the same root priority, the access point with the highest Ethernet address becomes the super root.

EXAMPLE:

Figure 3-6 shows an example of the super root selection process. Access points A and B have root priority "3." Access point C has root priority "5." Each access point has a unique Ethernet address.

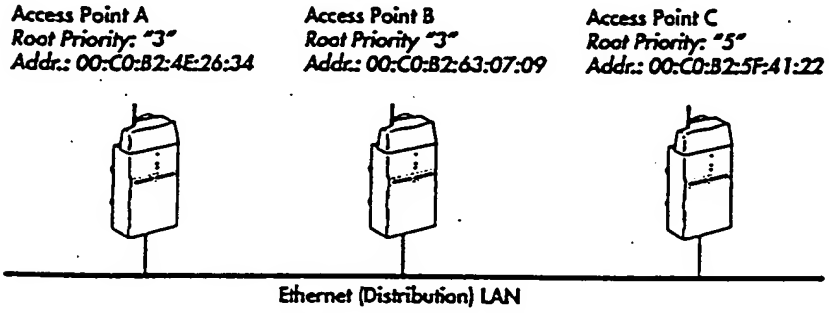


Figure 3-6
Super Root Node Selection Example

Access point C is the super root because it has the highest root priority. If access point C went offline, access points A and B would become super root candidates. However, because B's address is higher than A's, B would become the new super root.

Norand assigns a default value of "1" to the root priority. You can change this value through the access point's configuration menus to achieve a more efficient configuration for your site.

Directing Super Root Selection

Multiple root priority levels prioritize super root selection, which you specify and which is based on location. To direct the selection in networks with more than one super root candidate, you set the root priority of the preferred access point higher than the root priorities of the other access points. When two or more access points are operating in a single network, they constantly communicate to ensure only one super root exists.

Root priority is important if the super root goes offline or is disconnected from the distribution LAN. In this case the spanning tree autoconfigures and selects a new super root. How quickly it makes the selection depends on network size.

Typically, a network is operational within 2 to 3 minutes of when the super root goes offline. Multiple root node candidates allow for *redundancy*, which is the ability of a duplicate device to take over the function of another device.

If you install additional access points, the one with a root priority higher than the current super root's root priority immediately becomes the new super root when it attaches (associates) with the network. A network typically resumes operation within 2 to 3 minutes of when a new super root node is introduced. If several super root candidates have the same root priority, time to operation may increase while the system searches for the candidate with the highest Ethernet address.

Speeding Super Root Selection

Norand recommends that you set the root priority to a nonzero value for two super root candidates on small networks and two or three candidates on large networks. For example, on a small network two access points could have a root priority of "5"; other access points should have a root priority of "0." For convenience, you should assign the highest root priority to the access point that is the most physically accessible. You should also configure network-wide parameters (for example, flooding levels) consistently on all root node candidates.

Designated Bridge

Access points physically connected to a secondary physical LAN, and within the radio coverage area of an access point on the distribution LAN, are candidates to become the *designated bridge* for the secondary LAN. The designated bridge is a particular access point assigned the role of bridging frames destined for or received from the secondary LAN, providing a wireless connection between two unconnected secondary LAN segments.

The secondary LAN can be in the same building as the distribution LAN or in a separate building. Figure 3-5 on page 3-8 shows a single secondary Ethernet LAN.

Currently, an access point with the 900 MHz or UHF radio option can be a designated bridge. For a 2.4 GHz solution, two interbuilding bridges provide similar point-to-point capability by linking Ethernet LANs.

See Section 4, "Network Configurations," for an example of a configuration with interbuilding and intrabuilding bridges. Appendix B, "Recommended Network Products," lists the interbuilding bridge Norand suggests for use with the open system.

Designated Bridge Selection

If a network has one designated bridge candidate, that candidate becomes the designated bridge for the secondary LAN. If a network has two or more candidates, the candidate with the highest *bridge priority* automatically becomes the designated bridge. The range of bridge priorities is "0" through "7," where "7" is the highest bridge priority. An access point with bridge priority "0" cannot become a designated bridge.

EXAMPLE:

Figure 3-7 shows an example of the designated bridge selection process. The two access points connected to the secondary LAN have different bridge priorities ("3" and "5"). Access point B is the designated bridge because its bridge priority is higher than A's priority.

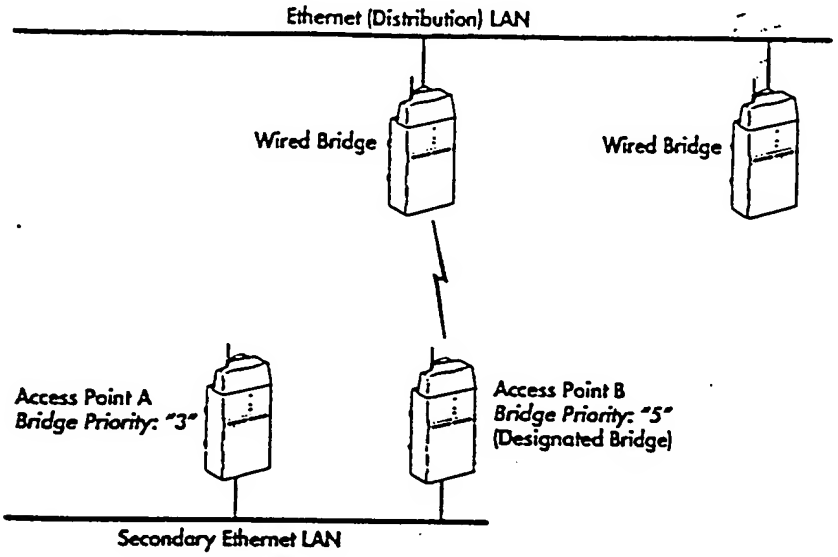


Figure 3-7
Designated Bridge Selection Example

If an access point on the secondary LAN has a higher bridge priority than other access points on the secondary LAN, but is outside the radio coverage area of an access point on the distribution LAN, it cannot become the designated bridge.

Norand assigns a default value of "1" to the bridge priority. If you are installing a designated bridge, you should change this value through the access point's configuration menus to determine the selection of the designated bridge.

If two or more access points have the same bridge priority, the access point with the highest Ethernet address becomes the designated bridge.

You must set a secondary *bridge flag* for the designated bridge's Ethernet port in addition to the bridge priority. Bridge flags allow the designated bridge to be configured to optimize which frame types are bridged over the wireless link. Bridge flags are unicast and multicast flooding options, discussed later in this section.

If a designated bridge goes offline, the remaining candidates determine which one becomes the new designated bridge. The designated bridge is always the access point that meets these criteria:

- Physically connects to a secondary Ethernet LAN
- Is within the radio coverage area of an access point on the distribution LAN
- Has the highest nonzero bridge priority; if it has the same bridge priority as another access point, then it has highest Ethernet address (unless the access point with the highest priority is out of range)
- Has a secondary bridge flag set for its Ethernet port

Configurations

Section 4 shows examples of secondary and multiple secondary LANs.

Secondary Proxim LAN

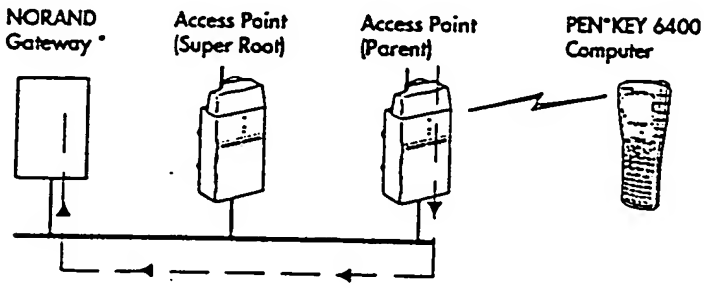
The radio coverage area of an access point with the Proxim 2.4 GHz radio option is a *secondary Proxim LAN*. The designated bridge is the access point with the radio. Default values for access points with the Proxim 2.4 GHz radio are factory-set to enable designated bridging, with flooding disabled.

Wireless Stations

Wireless stations are the end nodes in the spanning tree. Access points forward frames to and receive frames from the wireless stations. When a wireless station is power managed the access point buffers outbound messages and uses a pending message list to communicate that messages are buffered.

Unicast, broadcast, and multicast addresses are supported. A *unicast address* is a unique Ethernet address assigned to a single station. *Broadcast* is a transmission to all wireless stations at the same time. *Multicast* is a form of broadcast through which copies of the frame are delivered to a subset of all possible destinations with a common multicast address.

The wireless station converts, then sends to its parent, information it collects through its keyboard or scanner, for example. If an emulation solution requires a gateway, the gateway forwards the data to the host. Figure 3-8 shows data flow from a terminal emulation station to its parent and then to a NORAND gateway. Dashed lines are data.



* RC4030E Gateway, Wireless Network Access Server on host, 6950 Enterprise Gateway Server, or 6910 Integrated Gateway/Access Point

Figure 3-8
Sample Network Data Flow

LAN Identification Number (Domain)

So they can communicate, open wireless LAN nodes must have the same *LAN ID* (also called *domain*). It may be desirable to have independent networks operating with an overlapping radio frequency (RF) coverage area. In this case, you must set the LAN ID to ensure each network's access points and wireless stations communicate within their own network.

You set the LAN ID through configuration menus for each access point and wireless station. Norand assigns a default LAN ID of "0" to these devices. If you need to change this number to achieve a more efficient configuration for your site, you must change the number for each access point and wireless station in the same network to the new number. Norand strongly recommends that you change the default LAN ID to another value when you initially configure the devices.

▶ NOTE: *For the 900 MHz and UHF radio options, the range of LAN ID numbers is "0" through "254." For the Proxim 2.4 GHz radio option, the range is "0" through "15." (The LAN ID is the Proxim domain ID modulo 16.)*

Netname and Security ID

For link security, the wireless infrastructure provides a network naming capability called *netname*. For the Proxim 2.4 GHz radio option an additional parameter called *security ID* provides separate security to prevent unauthorized PC-compatible computers from associating with access points. (*Associating* is the process a wireless station follows to connect with a single access point at any one time.) Norand supports the security ID for the Proxim 2.4 GHz radio in addition to netname for compatibility with standard Proxim drivers in wireless stations.

Netname and security ID are ASCII strings. You set the strings through configuration menus for the access point and PC-compatible computer. The default netname is blank; the default security ID is "norandowl." So they can communicate, all access points and PC-compatible computers in the same network must have the same netname or security ID, or both. An access point or PC-compatible computer attaches to the network only if its netname or security ID matches the super root's netname or security ID.

Autoconfiguration

For most installations, one of the features of the open wireless LAN is its ability to automatically configure the spanning tree using factory default parameters of the access points.

Within minutes of when access points power up, the network discovers all possible communication paths, develops the spanning tree, and selects the super root. The spanning tree creates a loop-free network topology.

For the network to autoconfigure, Norand suggests that a minimal number of parameters be set:

- Root priority
- LAN ID
- Netname
- Bridge priority for each designated bridge
- For Proxim 2.4 GHz radio option: security ID

Norand also suggests that a minimal number of radio-specific parameters be set:

- For Proxim 2.4 GHz radio: channel and subchannel
- For 900 MHz radio: mode and channel
- For UHF radio: frequency

EXAMPLE 1:

Figure 3-9 shows an example of autoconfiguration. Each access point has the default root priority, LAN ID, and netname or security ID (or both). Each access point has a unique Ethernet address:

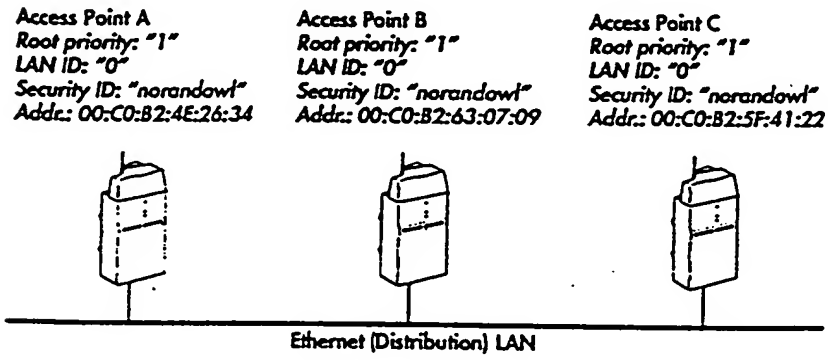


Figure 3-9
Autoconfiguration Through Ethernet Address

Access points A, B, and C are super root candidates because they have the same root priority. Access point B becomes the super root because it has the highest Ethernet address. If access point B went offline, access point C would become the super root because its Ethernet address is higher than access point A's address.

EXAMPLE 2:

Figure 3-10 shows another example of autoconfiguration. Each access point has the default LAN ID and netname or security ID (or both). Access points A and B have the default root priority. Access point C's root priority is "3." Each access point has a unique Ethernet address:

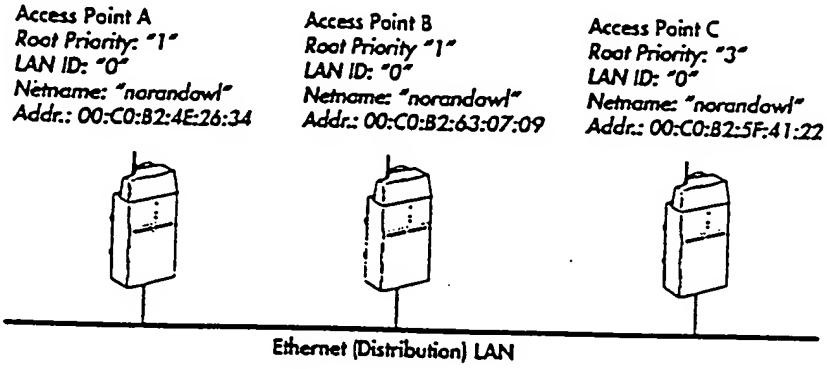


Figure 3-10
Autoconfiguration Through Root Priority

Access point C becomes the super root because it has the highest root priority. If access point C went offline, access points A and B would become super root candidates. B would become the new super root because its Ethernet address is higher than A's address.

Why Change the Spanning Tree Configuration?

The spanning tree can use factory-set default values for the autoconfiguration parameters to create a loop-free topology. However, those values might conflict with an adjacent LAN. To achieve a more desirable configuration, you can change the values through the access point's configuration menus.

Usually the best configuration depends on a network's particular characteristics and traffic loads. In configurations with secondary Ethernet LANs, the root priority and bridge priority can be changed to force a more efficient topology.

In this case the root priority should be set so that the distribution LAN is the "backbone" LAN. Norand or certified providers can review your needs to help you determine the best configuration for your environment.

Inter-Access Point Protocol

The open wireless LAN uses an inter-access point protocol to manage the wireless infrastructure. Open wireless LAN protocol frames are transmitted between NORAND network devices. The DIX Ethernet type of an open wireless LAN protocol frame is hexadecimal 875C.

Hello Frames

On Ethernet links, the super root or designated bridge periodically sends hello frames. On 900 MHz or UHF radio links, all access points periodically send hello frames. The frames help organize the access points into a spanning tree and advertise link availability.

Hello frames randomize around 1-, 2-, or 3-second intervals on an Ethernet link. The multicast destination 802 address for hello frames is always hexadecimal 01:C0:B2:4D:43:4F on Ethernet links.

On open wireless LAN radio links, hello frames can randomize around 1- or 2- second intervals. The interval is adjustable through configuration menus.

Power Management

For the 900 MHz or UHF radio option, the MACR sublayer provides several facilities to support sleeping wireless stations. A sleeping station initially synchronizes on a hello response frame from the wired bridge. Hello frames include a pending message list. Each entry in the list contains the node ID of a wireless station with pending messages. The wireless station calculates the time of the next expected hello response frame and powers down with an active timer interrupt set to wake it just before the next hello response frame is transmitted.

Power management extends the operating period for a given battery charge. By awakening before the next scheduled message, the wireless station misses no messages during a sleep period.

The Proxim 2.4 GHz radio option has a power management mechanism similar to the 900 MHz and UHF radio options. Norand supports the standard Proxim power management facilities for compatibility with the Proxim operating system or standard Proxim drivers in wireless stations.

Attach Frames

Open wireless LAN nodes periodically send unicast attach frames to explicitly associate with the open wireless LAN and refresh connections. Periodic attachment reduces or eliminates the need to flood unicast frames into the radio network.

Data Frames

Data frames normally bridge onto an Ethernet link as regular Ethernet frames with a DIX, 802.3, or SNAP protocol type. The 802 source address of NORAND open wireless LAN frames (DIX 875C) is always the 802 address of the access point that transmitted the frame, which is DIX, 802.3, or 802.3 SNAP over the Ethernet physical medium.

EXAMPLE:

A DIX IP frame originating on a radio link bridges onto an Ethernet link with a DIX type of hexadecimal 0800. The 802 source address is the address of the wireless station that originated the frame.

Optionally, you can disable bridging on an access point through its configuration menus. An access point with bridging disabled is a *wired access point* that will not convert Ethernet frames to open wireless LAN frames, and open wireless LAN frames to Ethernet frames. Normally, bridging should not be disabled.

MAC-R Frames

DIX Ethernet frames are used for inter-access point (MAC-R) communications.

Frame Forwarding

The access point maintains a forwarding database with an entry for each node in the subtree rooted at the access point, and entries for inbound nodes or nodes on the distribution LAN. All access points receive frames on the Ethernet link in *promiscuous mode*, which means an access point receives all broadcast frames and frames destined for unicast or multicast addresses. If the destination is in the subtree rooted at an access point, that access point forwards the frame outbound, for example. Otherwise the frame is ignored.

Optionally, flooding levels can be set so that frames are flooded throughout the network if the destination is unknown. Flooding is discussed later in this section.

The database associates unicast Ethernet addresses with *ports*. Each entry contains a destination address and an associated port identifier. When the access point receives a frame, it searches its forwarding database to determine the port of the destination. If the access point finds the destination and if the destination is on another port (other than the one on which the frame arrived), the access point bridges or forwards the frame to the destination port.

With bridging enabled, an access point bridges inbound open wireless LAN frames onto its Ethernet port if the destination is not in its forwarding database. If the destination is in its subtree, the access point bridges a frame from its Ethernet port outbound into the open wireless LAN radio network. An open wireless LAN frame is *inbound* if it is moving toward the super root. The frame is *outbound* if it is moving away from the super root.

EXAMPLE 1:

Figure 3-11 shows how spanning tree nodes route a frame. Dashed lines represent branches. Assumptions are as follows:

- Computer A is sending a unicast IP frame to computer B.
- Each access point and PEN*KEY computer has the 900 MHz or UHF radio option.

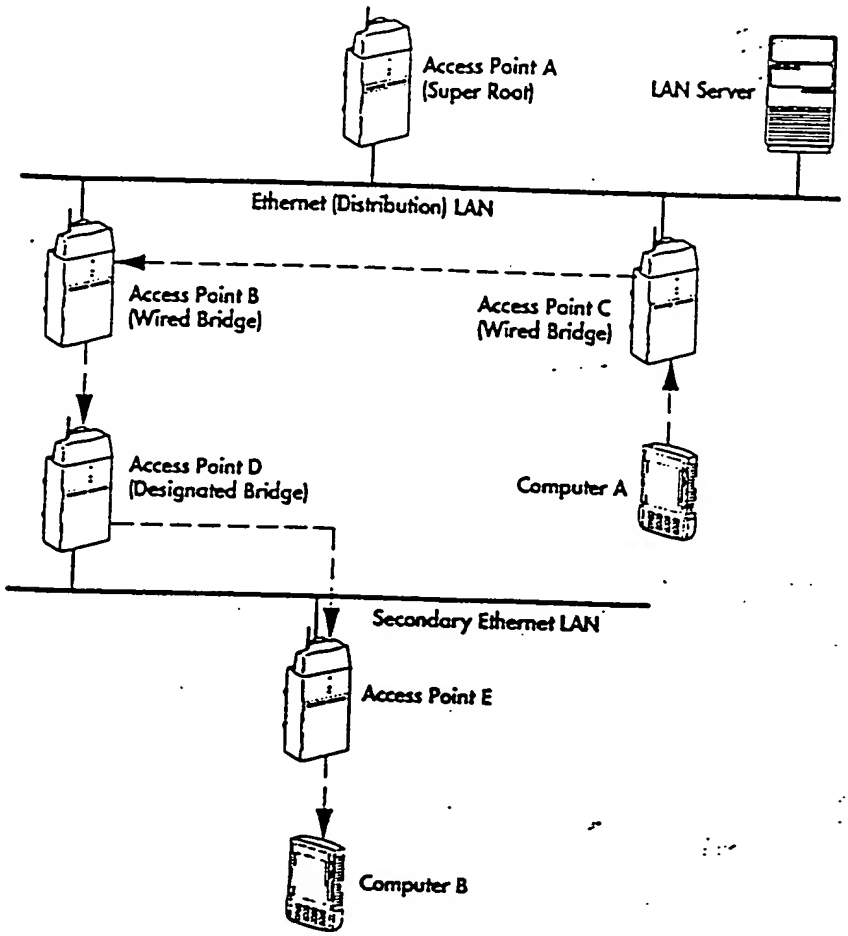


Figure 3-11
Frame Forwarding Between Wireless Stations

Spanning tree nodes route the frame as follows:

1. Computer A sends the unicast IP frame to its parent (access point C) through a wireless link.
2. Access point C bridges the frame onto the distribution LAN. The source and destination addresses are the 802 addresses of computers A and B, respectively. If the frame is DIX, the Ethernet type is 0800.
3. Access points A and B receive the bridged frame. In this case, the super root (access point A) and access point B should have a route table entry for computer B. However, the root entry for the access points' private database is marked as *distributed*. (Distributed means another access point is responsible for bridging outbound frames to the destination.) The super root will not bridge a non-open wireless LAN frame if its route table entry for the destination is distributed.
4. Access point B bridges the IP frame and forwards it over its radio port to access point D. Access point D has a distributed table entry for computer B. Therefore, access point D bridges the frame onto the secondary Ethernet LAN (that is, as a DIX IP frame).
5. Access point E receives the frame because its Ethernet port is in promiscuous mode. Access point E has a route table entry for computer B.
6. Access point E bridges the frame from Ethernet and forwards it over its radio port to computer B.

EXAMPLE 2: If computer B sends an IP frame to the LAN server on the distribution LAN, Figure 3-12 shows how spanning tree nodes route the frame.

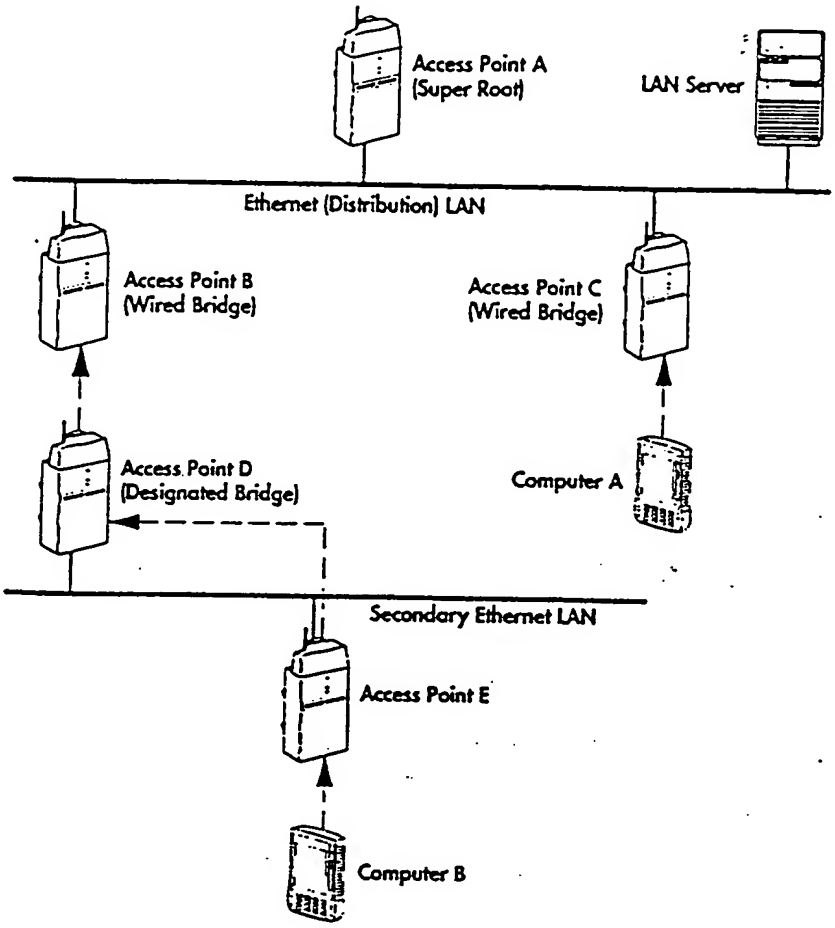


Figure 3-12
Frame Forwarding Between Wireless Station and LAN Server

Spanning tree nodes route the frame as follows:

1. Computer B sends the frame to its parent (access point E) through a wireless link.
2. Access point E bridges the frame onto the secondary Ethernet LAN as a IP frame. Note that if the LAN server was connected to the secondary LAN, the server would receive the bridged frame.
3. Access point D forwards the frame inbound to access point B.

4. Access point B bridges the frame onto the distribution LAN as an IP frame. If the frame is DIX, the Ethernet type is 0800.
5. The server receives the frame. Forwarding is transparent to the server, which has an Ethernet protocol stack.

Flooding

If the access point is unable to find a destination address in its forwarding database (the destination is unknown), the access point floods the frame if configured to do so. *Flooding* is a process where frames received on one port are transmitted on all other ports.

You can configure unicast or multicast flooding options (or both) for the distribution LAN and for each secondary Ethernet LAN. You configure flooding options through the super root's configuration menus. Because access points with a nonzero root priority are candidates to become the super root, each access point with a nonzero root priority should have the same flooding options for consistency.

In many cases flooding puts unnecessary traffic onto the RF medium. For this reason, the default configuration for the access point disables outbound flooding of unicast frames.

To reduce traffic you can limit flooding to a subset of secondary Ethernet LANs. This feature is intended for sites with a mixture of secondary Ethernet LANs and secondary Proxim LANs. Depending on your application, you may want to avoid flooding frames to secondary Proxim LANs but want to flood frames to certain secondary Ethernet LANs.

You can selectively flood the frames by specifying a secondary bridge flag for each secondary LANs' designated bridge. The bridge flag works in conjunction with the flooding levels set for the super root. The designated bridge for a secondary LAN notifies the super root and each access point on the inbound path to the super root that it requires unicast or multicast flooding, or both.

Access points connected to the secondary Ethernet LAN and with a nonzero bridge priority are candidates to become the designated bridge. For consistency, the same flooding options should be set for each candidate.

Complete instructions on how to configure flooding options are in the *6710 Access Point User's Guide (NPN: 961-047-081)* and *6910 Integrated Gateway/Access Point User's Guide (NPN: 961-047-095)*.

Unicast Flooding Options

You can configure the access point to take one of the following actions when it receives unicast frames:

- Discard unicast frames that originate on the distribution LAN if the destination is unknown. The access point forwards unicast frames that originate in the radio network inbound, until the frame arrives at an access point with a route entry for the destination. The access point relays an inbound unicast frame onto the distribution LAN if the destination is unknown.
- Flood unicast frames to the distribution LAN and to each secondary Ethernet LAN that has unicast flooding enabled. For example, an access point forwards, to the distribution LAN and to each secondary Ethernet LAN that has unicast flooding enabled, a unicast frame that originates in the radio network if the destination is unknown.
- Flood unicast frames to the distribution LAN and all secondary Ethernet LANs if the destination is unknown.

Generally, the best option is to disable unicast flooding. However, flooding of unicast frames is required if the network contains one or more secondary Ethernet LANs with wired stations that do not periodically generate traffic.

Multicast Flooding Options

You can configure the access point to take one of the following actions when it receives multicast frames:

► NOTE: *Selecting higher multicast flooding levels increases wireless LAN traffic.*

- Discard multicast frames that originate on the distribution LAN.
- Forward, to secondary Ethernet LANs that have multicast flooding enabled, multicast frames that originate on the distribution LAN.

- Flood, throughout the open wireless LAN, multicast frames that originate on the distribution LAN. The access point forwards, to the distribution LAN, multicast frames that originate in the radio network or on a secondary Ethernet LAN.
- Flood, throughout the open wireless LAN, all multicast frames. For example, if a multicast frame originates in the radio network, the access point forwards the frame to the distribution LAN and to each access point on the open wireless LAN. An access point broadcasts the message on each radio port and relays the message to any attached secondary Ethernet LAN.

▶ NOTE: *Broadcast DIX Address Resolution Protocol (ARP) frames (DIX type is hexadecimal 0806) are always forwarded to each access point on the open wireless LAN, even when you set no multicast flooding options.*

Filtering

You can define filtering options to selectively discard Ethernet frames the access point receives on its Ethernet port. *Filtering* is a process that allows only predefined frame types to be forwarded. Filtering prevents the access point from forwarding unnecessary Ethernet frames onto the radio network.

Two filtering options are available: DIX Ethernet and programmable. Complete instructions on how to configure both options are in the *6710 Access Point User's Guide (NPN: 961-047-081)* and *6910 Integrated Gateway/Access Point User's Guide (NPN: 961-047-095)*.

DIX Ethernet Filtering

You can enter a list of up to 15 DIX Ethernet frame types through access point configuration menus. If the list of types is set to "enabled," Ethernet frames with frame types equal to those in the list are forwarded from the Ethernet physical medium to the access point bridging modules. All other frames are discarded. Frame types 875C (open wireless LAN), 0800 (IP), and 0806 (ARP) are always enabled.

If the list of types is set to "disabled," Ethernet frames with frame types equal to those in the list are discarded. Other frames are forwarded to the access point bridging modules within the constraints of any other filtering options.

Filter lists enhance the performance of the access points by keeping unwanted Ethernet frames from being handled and forwarded by the access points. For this reason DIX Ethernet filtering is the preferred filtering option.

The DIX frame type is the two bytes after the source address in an Ethernet MAC header. In the IEEE 802.3 standard the bytes represent the length of the Ethernet frame. Therefore, the DIX Ethernet filtering option is of limited use in 802.3 networks.

Programmable Filtering

You can program unicast or multicast filters (or both) through access point configuration menus. Programmable filters are mainly useful for selectively filtering multicast frames, since the destination address cannot be associated with a single station. That is, the frame must be flooded.

A pattern list and an expression with enabled or disabled masks form the access point's filter. Each pattern list has a fixed size and frame offset. Each list can join to another list through AND, OR, and other operators to build complex filters.

EXAMPLE: You can define a filter to forward only broadcast Novell Service Advertisement Protocol (SAP) frames from a select group of servers. You can also filter all multicast frames except for ARP requests from a group of servers.

Processes

The flowchart in Figure 3-13 summarizes the filtering and flooding processes when the access point receives a unicast frame.

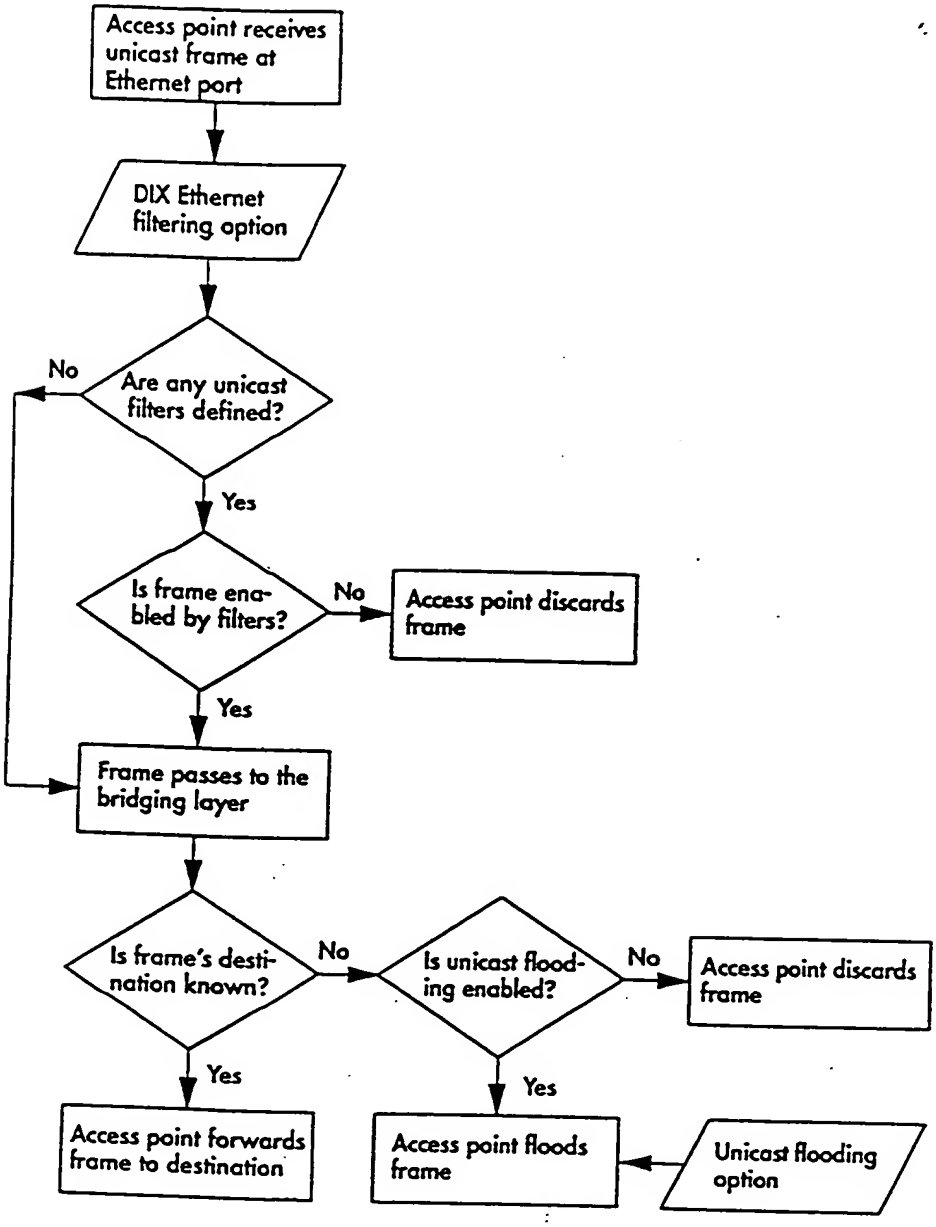


Figure 3-13
Filtering and Flooding Processes

Inter-Access Point Communications

Access points learn the locations of wired and wireless stations through a spanning tree. Because spanning tree information is communicated at the MAC sublayer, access points cannot communicate across IP routers, which connect separate IP subnets. Inter-access point communications at the MAC-R sublayer are not routable.

If an IP router is present, you can enable inter-access point communications by configuring the router to bridge DIX type 0875C packets. Consult a Norand Systems Engineer for more information about enabling bridging on routers.

EXAMPLE: In the configuration example in Figure 3-14, access points on subnet A cannot communicate with access points on subnet B:

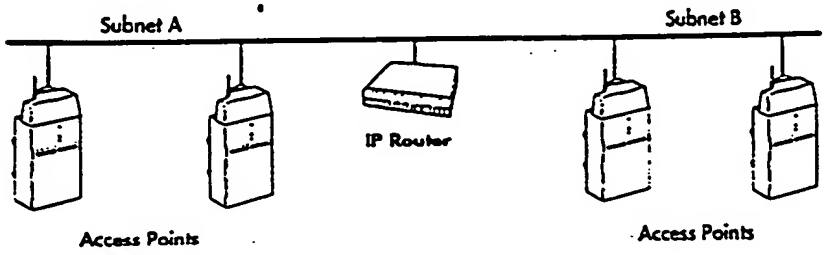


Figure 3-14
Inter-Access Point Communications

See Section 8, "Installation," for general information about routers.

Roaming

An open wireless LAN typically contains multiple access points, which provide an extended, seamless radio coverage area. The coverage areas of multiple access points must overlap to provide uninterrupted wireless access to the Ethernet medium.

Overlapping coverage areas enable a wireless station to move from the coverage area of one access point into the area of another while maintaining LAN connectivity. Wireless stations monitor the reliability of communications with an access point and initiate roaming if a significantly better link can be established with another access point.

Reassociating With Another Access Point

When a wireless station detects it has roamed, it must reassociate with another access point. When the wireless station connects with another access point, the new access point updates its forwarding database and forwards the update to the super root, which forwards it to the previous access point. This updating process ensures frames are sent along the proper branches of the spanning tree to connect to the wireless stations.

When a wireless station roams between access point coverage areas, the new access point begins forwarding frames to the wireless station. The previous access point stops forwarding. A wireless station with the 900 MHz or UHF radio option listens for hello frames on the network and then requests connection to the node with the fastest route to the distribution LAN. The route is determined by the *cost*. The cost in the hello frame is generally an indication of the bandwidth cost to reach the distribution LAN.

As wireless stations roam through the open wireless LAN, they must establish a connection with a single access point (the parent) as their entry point to the wired Ethernet backbone at any one time. When a wireless station approaches a coverage area boundary, it searches for an access point with a better signal and more reliable data throughput.

Updating the Forwarding Database

An access point updates its forwarding database when it receives a frame on a primary or secondary LAN port. The access point makes or updates an entry containing the 802 source address and the source port. If the new source port differs from the previous one, the access point changes its database to indicate the wireless station has roamed from one physical segment to another.

Attach frames on open wireless LAN ports update the forwarding database. The frames are sent each time a wireless station roams, and are periodically sent to maintain the path. Frames are always forwarded to the super root, which generates a detach frame to delete the old path when a wireless station roams.

Use of Bridges Within the Infrastructure

The open wireless LAN architecture is designed to operate correctly when off-the-shelf transparent bridges are used within the Ethernet backbone.

EXAMPLE: The configuration example in Figure 3-15 shows a PEN*KEY computer roaming to an access point on the other side of an off-the-shelf bridge:

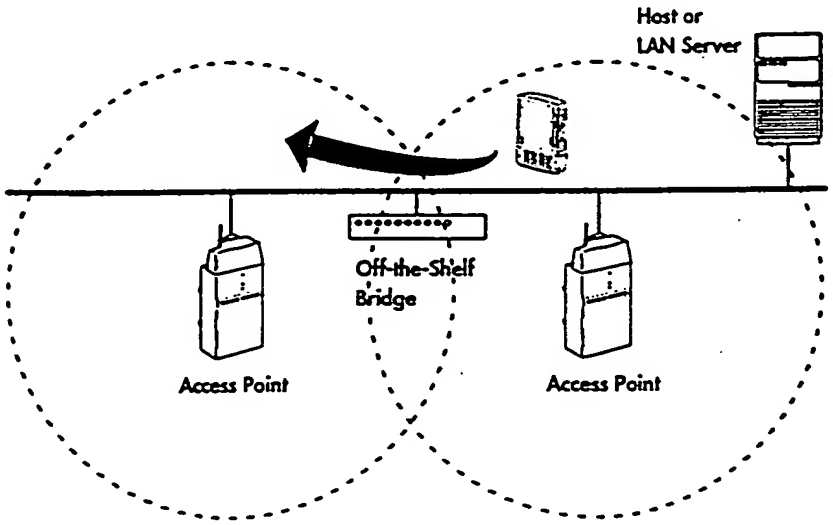


Figure 3-15
Off-the-Shelf Bridge Within Infrastructure

For more information about how bridges operate in general, see Section 8. Appendix B lists network products, including bridges, that Norand recommends.

Section 4

Network Configurations

About This Section

This section shows examples of network configurations with the 900 MHz, UHF, and Proxim 2.4 GHz radio options.

Configurations With 900 MHz, UHF, or Proxim 2.4 GHz Option

Configurations with the 6710 Access Point with the 900 MHz, UHF, or Proxim 2.4 GHz radio option include the following (described on the following pages):

- Configuration with PC-compatible computers
- Configuration with multiple access points.
- Hybrid configuration
- Configuration with remote network management station
- Configuration with TFTP server
- Configuration with RC4030E Gateway
- Modified star configuration
- Configuration with Wireless Network Access Server
- Configuration with 6950 Enterprise Gateway Server

PC-Compatible Computers

In this configuration the 6710 Access Point forwards, over the radio network, frames between PC-compatible computers and the LAN server or IP host (or both) on the Ethernet LAN. In the example shown in Figure 4-1, the access point forwards frames between a PEN*KEY® 6100 and notebook. To the host and server, these computers appear to be hard-wired to the LAN.

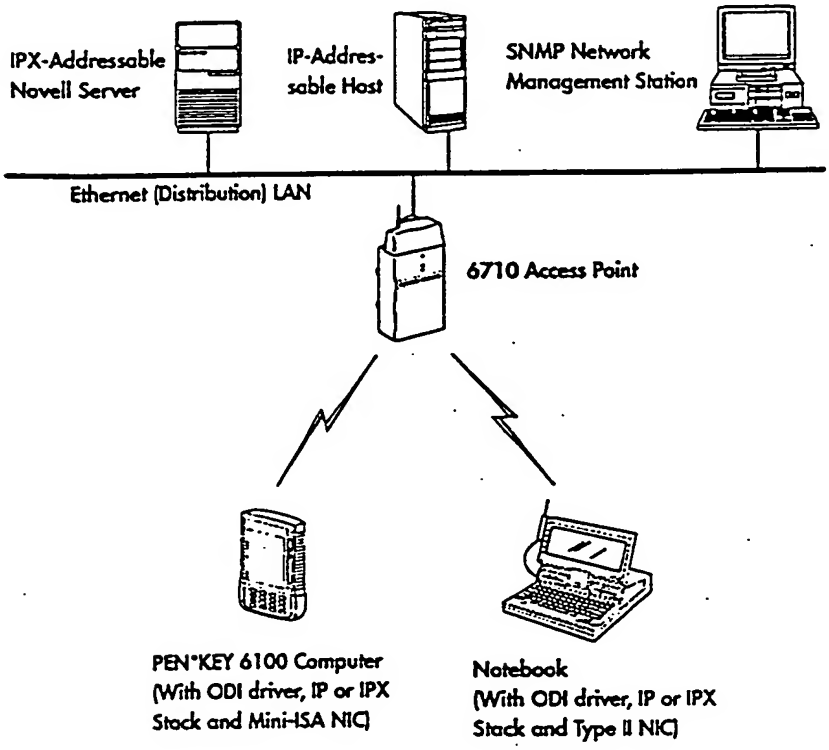


Figure 4-1
Configuration With PC-Compatible Computers

Multiple Access Points

Multiple 6710 Access Points can bridge frames between wireless stations and the Ethernet LAN (Figure 4-2). The open wireless LAN infrastructure enables the wireless stations to roam from the coverage area of one access point to another coverage area without disrupting network service. Roaming is seamless and transparent to the end user and application.

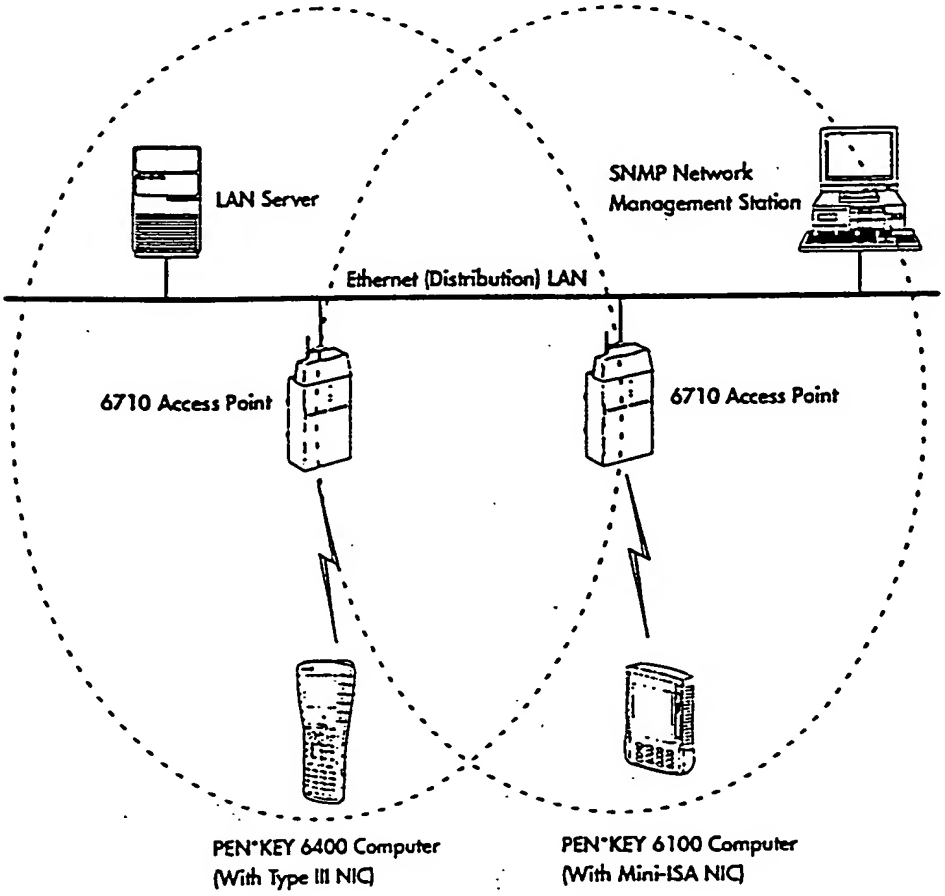


Figure 4-2
Configuration With Multiple Access Points

Hybrid

Different topologies connected together create a hybrid configuration, which results in a larger network span. Figure 4-3 shows a sample configuration with Token Ring and 10BASE2. The router divides the configuration into three separate networks: Token Ring, the company's enterprise network, and the hub with 6710 Access Points.

▶ NOTE: *Appendix B lists hubs and other recommended network products.*

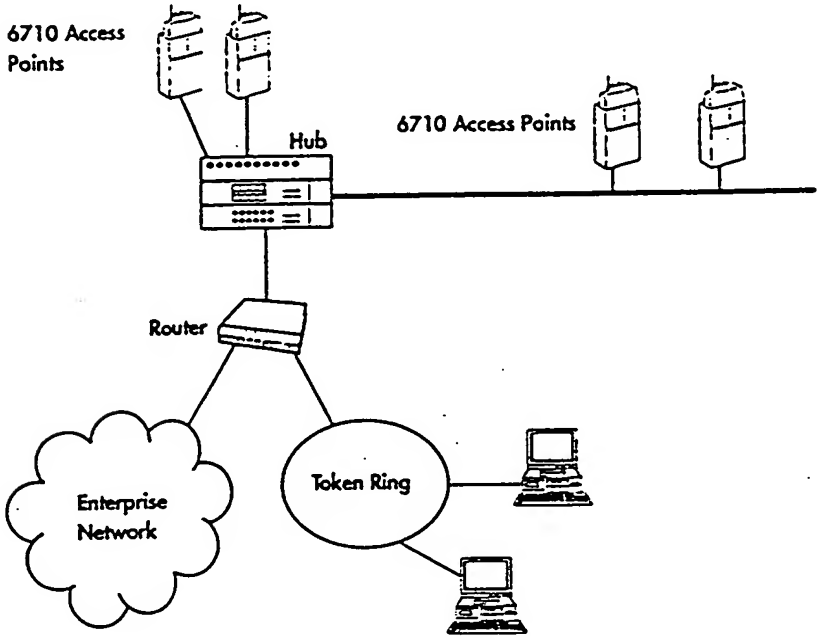


Figure 4-3
Hybrid Configuration

Remote Network Management Station

You can manage the wireless infrastructure through SNMP, which provides a way for network management platforms to query network devices for status and other device information. Figure 4-4 shows a sample configuration with a remote SNMP network management station. The connectivity solution shown is a remote access modem.

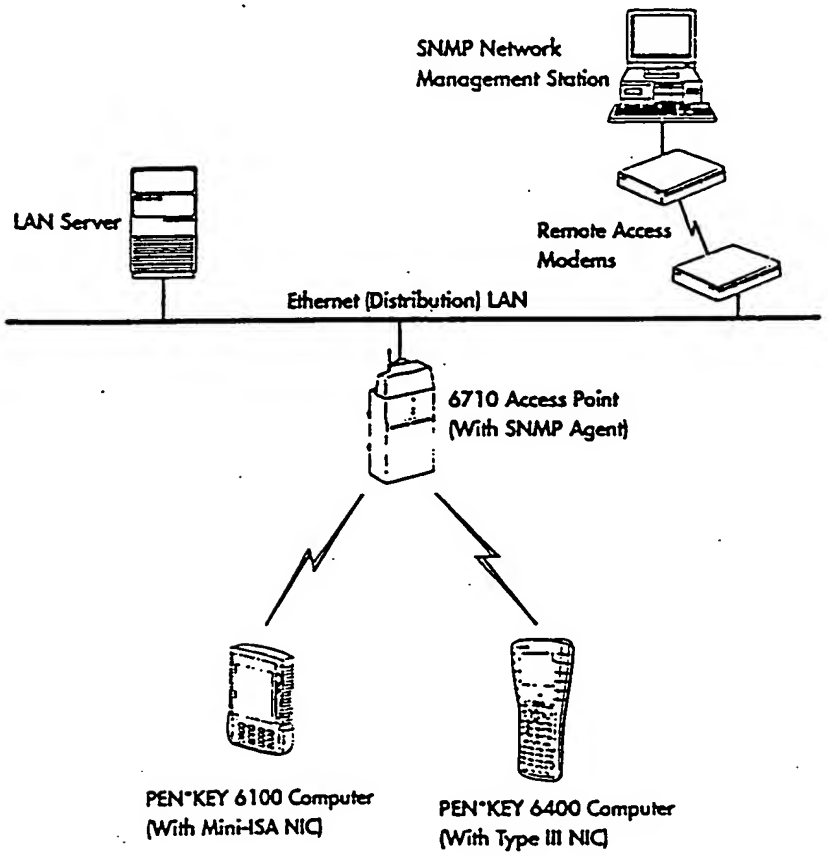


Figure 4-4
Configuration With Remote Network Management Station

PC TFTP Server

You can download the latest version of system software to a 6710 Access Point through a PC TFTP server. Connectivity solutions for the PC TFTP server are direct LAN and Ethernet modem.

Direct LAN

Figure 4-5 shows a PC TFTP server directly connected to the LAN. Each access point is a TFTP client you can access through a TELNET or SNMP session with the access point's IP address.

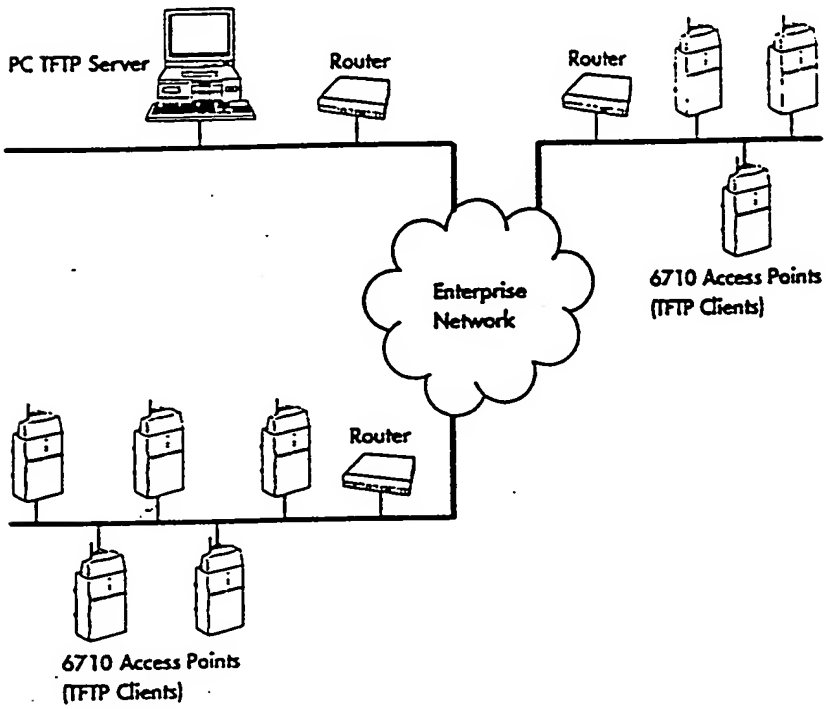


Figure 4-5
Configuration With PC TFTP Server, Direct LAN

Ethernet Modem

Figure 4-6 shows a PC TFTP server connected to an Ethernet modem. Each access point is a TFTP client you can access through a TELNET or SNMP session with the access point's IP address.

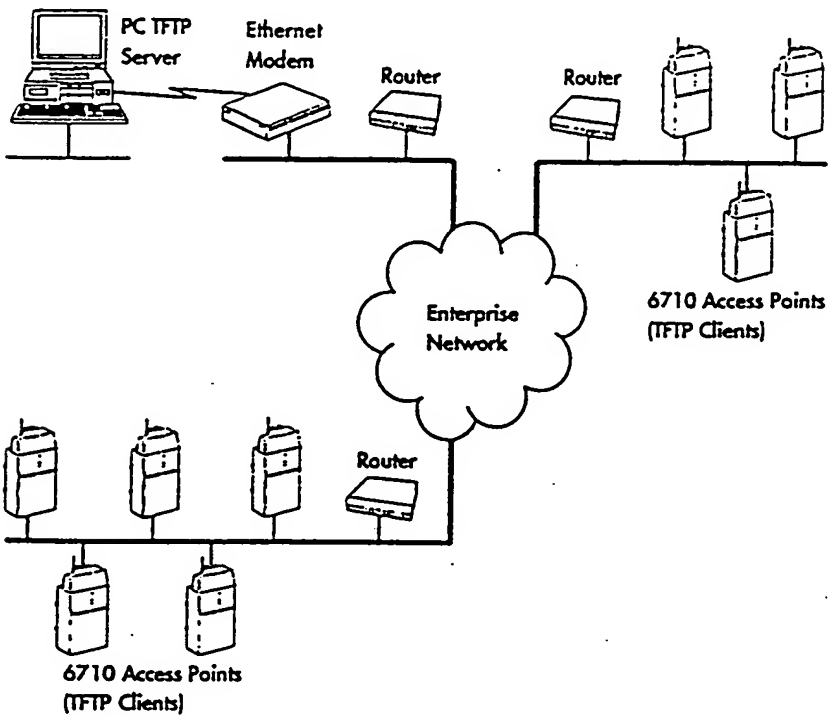


Figure 4-6
Configuration With PC TFTP Server, Ethernet Modem

RC4030E Gateway

Figure 4-7 shows a configuration with an RC4030E Gateway connected to a host running the 3270 or 5250 protocol. The 6710 Access Point forwards, over the radio network, data frames between the terminal emulation stations and the gateway. The gateway converts the data frames into the host protocol.

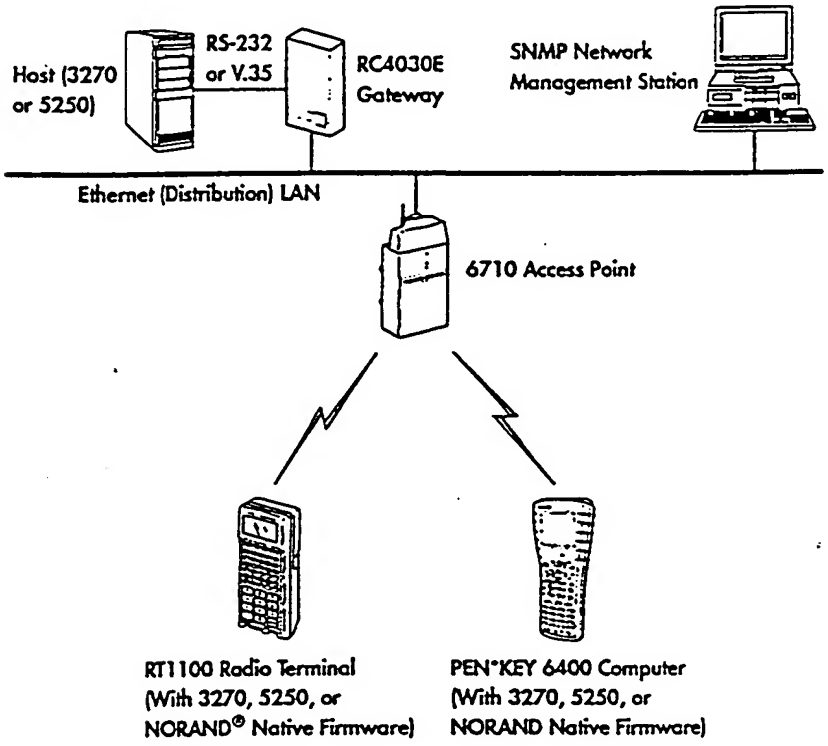


Figure 4-7
Configuration With RC4030E Gateway

Modified Star

Figure 4-8 shows 6710 Access Points and an RC4030E Gateway connected to stacked hubs. A fiber backbone connects the hubs. This configuration forms a modified star. For more information about how hubs and other network communication products operate in general, See Section 8, "Installation."

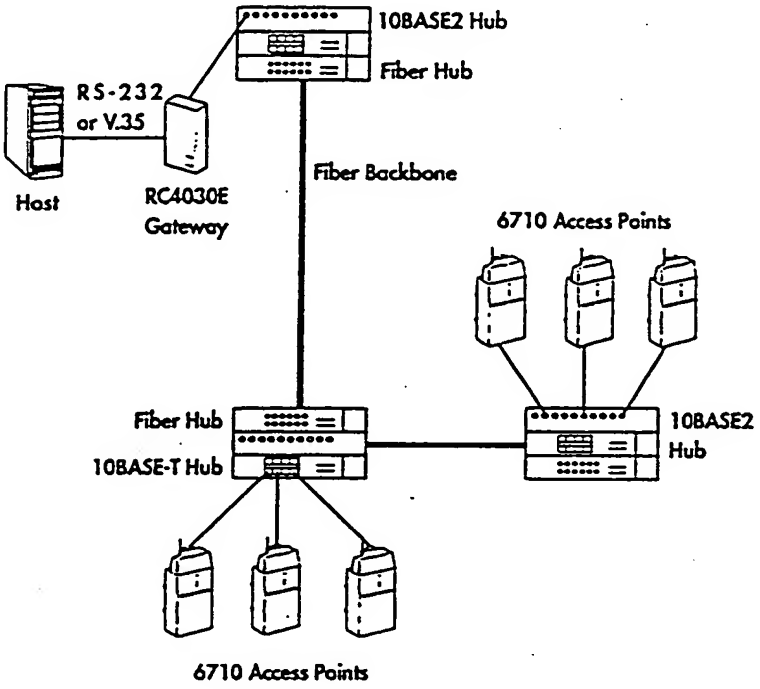


Figure 4-8
Modified Star Configuration

Wireless Network Access Server

Figure 4-9 shows a configuration with Wireless Network Access Server (WNAS) software running on an RS/6000 host. The 6710 Access Point forwards, over the radio network, data frames between the terminal emulation stations and WNAS on the host. WNAS converts the data frames into the TCP/IP TELNET protocol.

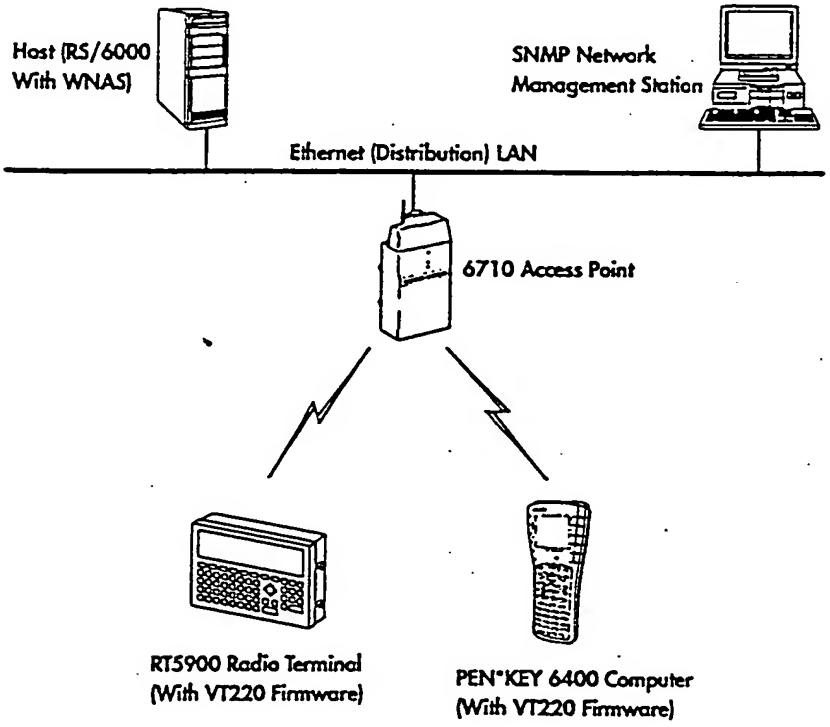


Figure 4-9
Configuration With WNAS

6950 Enterprise Gateway Server

Figure 4-10 shows a configuration with a 6950 Enterprise Gateway Server. The 6710 Access Point forward forwards, over the radio network, data frames between the terminal emulation stations and the gateway server. The gateway server converts the data frames into the TCP/IP TELNET protocol.

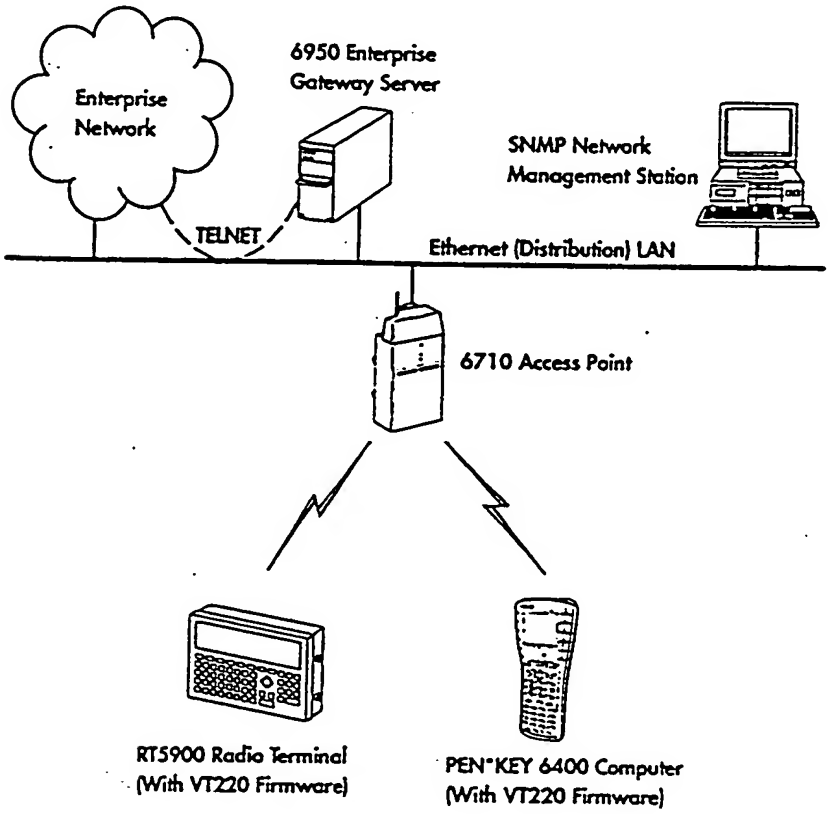


Figure 4-10
Configuration With 6950 Enterprise Gateway Server

Additional Configurations With 900 MHz or UHF Option

Configurations with the 6710 Access Point with the 900 MHz or UHF radio option include the following:

- Secondary LAN
- Multiple secondary LAN
- Wireless access point

▶ NOTE: *The UHF radio option is technically capable of being exercised in these configurations. However, because of bandwidth limitations, these configurations with the UHF radio option are not recommended except in special situations. Contact a Norand Sales Representative for more information.*

Secondary LAN

In a secondary LAN configuration, a designated bridge connects a secondary Ethernet LAN to the distribution LAN through a wireless link. The LANs can be in the same building or in separate buildings.

▶ NOTE: *In general, bridging through a wireless link has lower performance than wired Ethernet.*

Same Building

In the example shown in Figure 4-11 the access point is forwarding, over the radio network, frames between the LAN server and desktop B wired to a secondary Ethernet LAN.

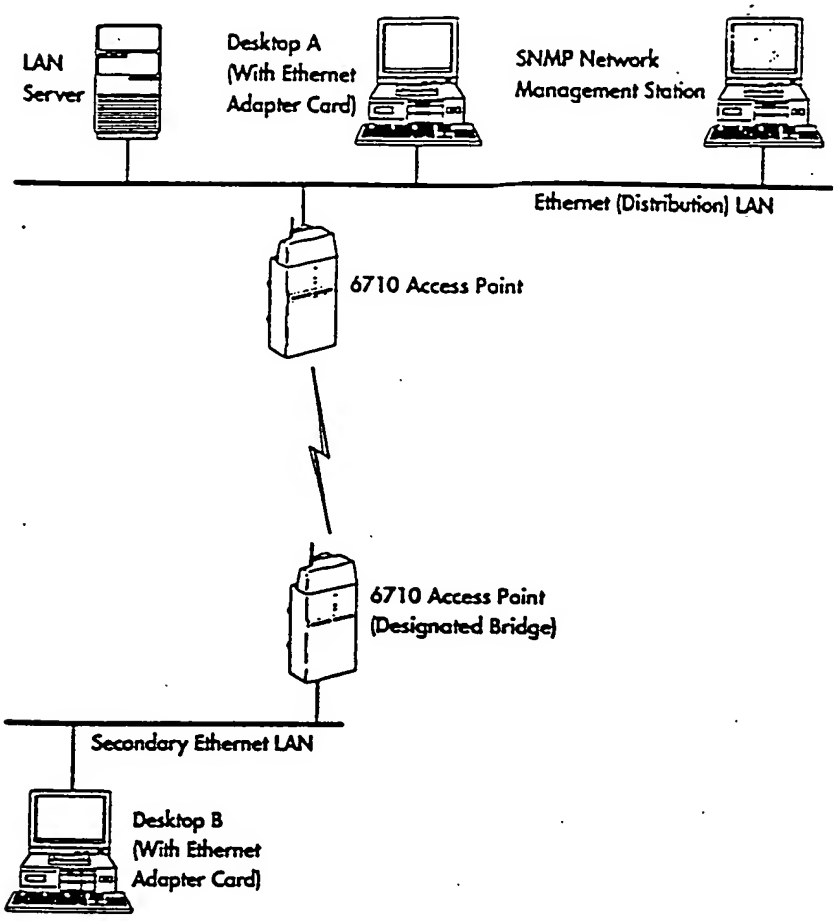


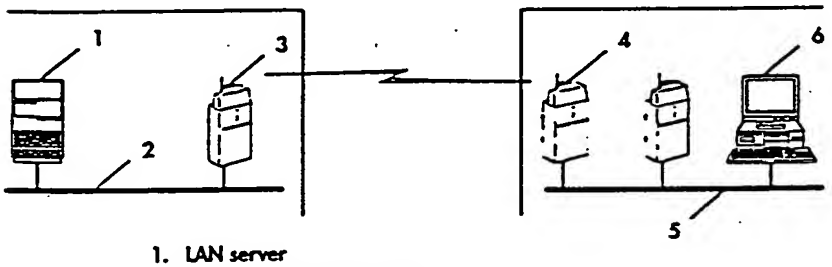
Figure 4-11
Secondary LAN Configuration, Same Building

Separate Buildings

Two access points with the 900 MHz or UHF radio option and standard antennas can connect two Ethernet LANs in separate buildings through a wireless link. This configuration eliminates the need to lay cables between the buildings or lease a line from the phone company. The access points also provide coverage for wireless stations that require connectivity to the LAN.

For best results, you should place the access points and antennas providing the wireless link near windows. Norand or certified providers can supply additional placement information through a formal site survey. For current information about standard antenna availability, consult a Norand Sales Representative.

Figure 4-12 shows a sample configuration where access points with the 900 MHz radio option are forwarding frames between the LAN server on the distribution LAN and the desktop wired to the secondary Ethernet LAN. For best results from the secondary Ethernet LAN, you should assign the highest bridge priority to the access point with the best physical link, which is the access point by the window.



1. LAN server
2. Ethernet (distribution) LAN
3. 6710 Access Point
4. 6710 Access Point (designated bridge)
5. Secondary Ethernet LAN
6. Desktop (with Ethernet adapter card)

Figure 4-12
Secondary LAN Configuration, Separate Buildings

Multiple Secondary LAN

In a multiple secondary LAN configuration, designated bridges connect secondary Ethernet LANs to the distribution LAN through wireless links. In the example shown in Figure 4-13, desktops A and B can communicate with other desktops on their own LAN, or with desktops on separate secondary LANs. The designated bridges forward frames between desktops A and B.

▶ NOTE: *In general, bridging through a wireless link has lower performance than wired Ethernet.*

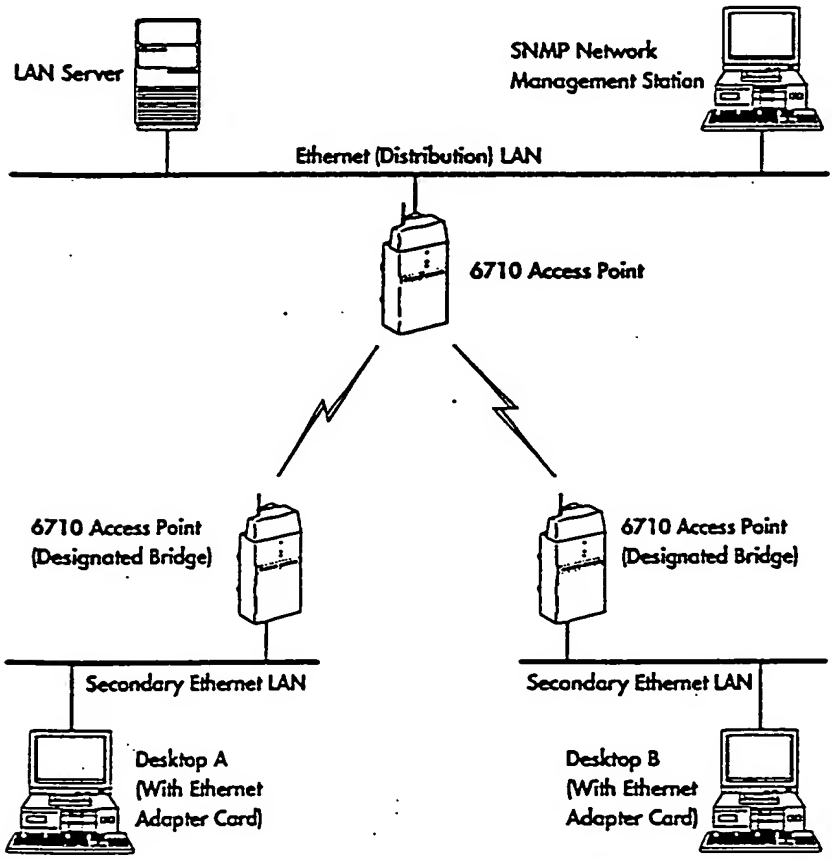


Figure 4-13
Multiple Secondary LAN Configuration

Wireless Access Point

A 6710 Access Point with the 900 MHz or UHF radio option can be a wireless access point that overlaps coverage with a wired bridge. In the example shown in Figure 4-14 the access points are forwarding frames between the wireless stations and the Ethernet LAN over the radio network. Note that the wireless access point does not physically connect to the Ethernet medium.

▶ NOTE: *In general, forwarding through wireless access points has lower performance than wired Ethernet. Section 7, "Wireless Access Points," covers wireless access points and performance issues.*

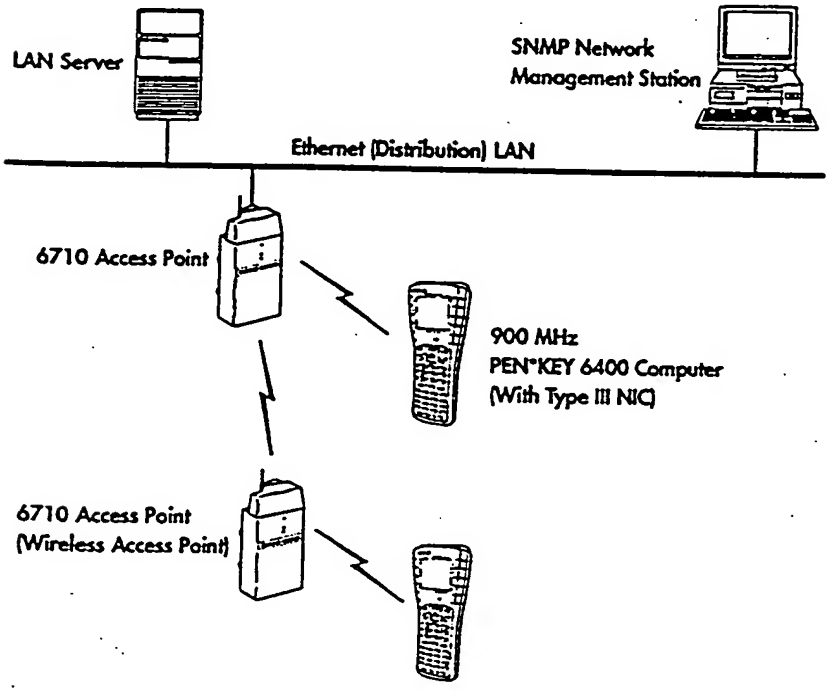


Figure 4-14
Configuration With Wireless Access Point

Additional Configurations With Proxim 2.4 GHz Option

PEN*KEY computers by Norand, and third-party PC-compatible computers with the Proxim 2.4 GHz radio option, are capable of wireless peer-to-peer (ad hoc) connections. The 6710 Access Point with the Proxim 2.4 GHz radio option can be a device in a point-to-point configuration with interbuilding bridges. The following pages describe these configurations.

Wireless Ad Hoc or Peer-to-Peer

A source wireless station establishing a radio link with a destination wireless station creates an ad hoc or peer-to-peer connection. This connection establishes a network that can share files and other resources instantly. Figure 4-15 shows two notebooks and one PEN*KEY 6100 Computer in a peer-to-peer configuration. The notebooks have Proxim 2.4 GHz Type II NICs. The PEN*KEY computer has a Proxim 2.4 GHz mini-ISA NIC in the pod unit attached to the back of the computer.

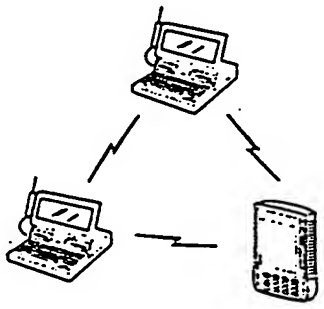


Figure 4-15
Wireless Ad Hoc or Peer-to-Peer Configuration

Point-to-Point

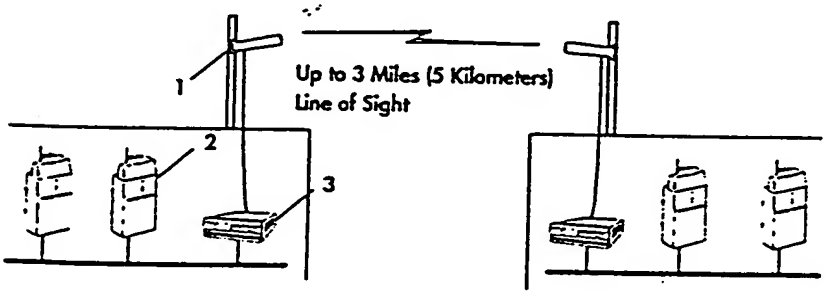
Two interbuilding bridges with high-gain, 2.4 GHz yagi (unidirectional) antennas can connect Ethernet LANs in two separate buildings through a wireless link. This point-to-point configuration eliminates the need to lay cables between the buildings or lease a line from the phone company.

▶ NOTE: *In general, bridging through a wireless link has lower performance than wired Ethernet.*

Each antenna has a range of up to three miles (5 kilometers) line of sight. For best results, you should properly mount each antenna onto an antenna mast or exterior wall. Norand or certified providers can provide additional placement information through a formal site survey.

6710 Access Points coexist with interbuilding bridges on the same Ethernet LAN. To the wireless infrastructure, separate Ethernet LANs with access points and interbuilding bridges operate as a wired network. The interbuilding bridge's architecture supports any protocol or network operating system that supports Ethernet.

Figure 4-16 shows a sample configuration with 6710 Access Points and interbuilding bridges.



1. Yagi antenna (on mast)
2. 6710 Access Point
3. Interbuilding bridge

Figure 4-16
Point-to-Point Configuration, Separate Buildings

Section 5

Network Connectivity

About This Section

Wireless NICs and NORAND® PC-compatible computers provide a range of network connectivity solutions. This section describes these network products and the solutions they provide.

Wireless NICs

NICs for wireless stations that require connectivity to the enterprise Ethernet LAN include the following:

- Type III
- Type II
- Mini-ISA
- ISA

These NICs conform to various PC card and ISA bus standards. To a host or server, wireless stations equipped with NICs appear to be standard network nodes wired to the Ethernet medium. By operating at the Data Link layer, the NICs provide protocol-independent access for mobile users into a wired Ethernet LAN.

► NOTE: *Appendix A, "Radio Options," contains wireless NIC specifications and features.*

Type III (900 MHz and Proxim 2.4 GHz)

The Type III wireless NIC (Figure 5-1) is a high-performance adapter for 6710 Access Points and PEN*KEY® 6100 (900 MHz radio option only), 6400, and 6600 Computers. For PEN*KEY computers the NIC supports ODI or NDIS drivers or both, which facilitate mobile applications in environments that support these drivers. For proper network communications, you must configure the NIC's software according to your site's requirements.

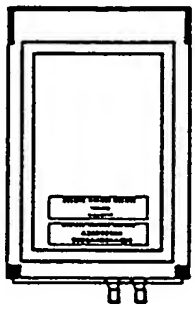


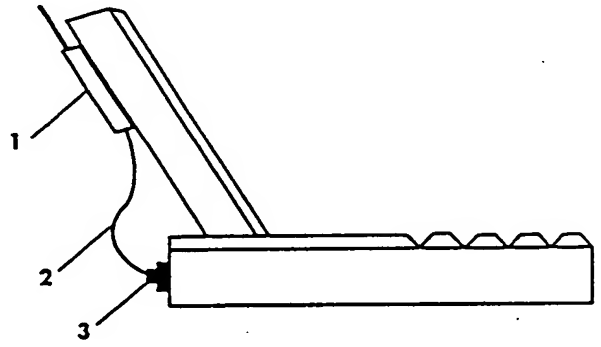
Figure 5-1
Type III Wireless NIC

The Type III NIC plugs into one of the 6710 Access Point's PC card-compatible slots and is field-replaceable. Norand preinstalls the NIC into the PEN*KEY computers; Norand or other qualified service personnel must replace the NIC for these computers.

Type II (Proxim 2.4 GHz)

The Type II wireless NIC is a high-performance adapter for laptop and notebook computers with Type II card slots. The Type II NIC supports ODI and NDIS drivers. Norand provides NIC software on diskette. For proper network communications, you must load the software into the computer and configure it according to your site's requirements.

The Type II NIC consists of a standard Type II card that plugs into the computer's card slot, and an antenna unit that connects to the card through a tether and plug. The antenna unit usually mounts onto the back or side of the computer. For best performance the antenna extends above the top of the notebook. Figure 5-2 shows a notebook with an installed Type II NIC.



1. Antenna unit
2. Tether
3. Plug

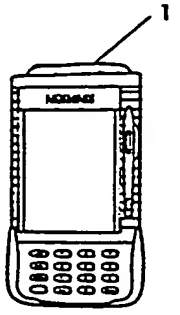
Figure 5-2
Notebook With Type II Wireless NIC

Mini-ISA (UHF and Proxim 2.4 GHz)

The mini-ISA wireless NIC is a high-performance adapter for wireless stations in these series: PEN*KEY 6100 Computers (pod solutions), RT1100 and RT1700 Radio Terminals (radio module solutions), and RT5900 Radio Terminals (internal solutions).

For the PEN*KEY 6100 Computer, the mini-ISA NIC supports ODI and NDIS drivers. For proper network communications, you must configure the NIC's software according to your site's requirements. Appendix C, "ODI and NDIS Driver Configurations," shows examples of driver configurations for a PEN*KEY 6100 Computer.

Norand preinstalls the mini-ISA NIC into the pod unit that attaches to the back of the PEN*KEY 6100 Computer (Figure 5-3). Because the NIC is installed in the pod, the computer's PC card slots are accessible for other uses.



1. Pod

Figure 5-3
PEN*KEY 6100 Computer Pod

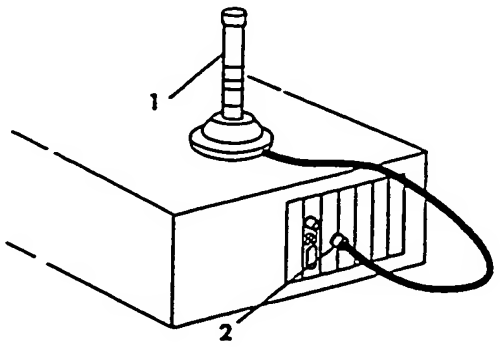
Norand preinstalls the mini-ISA NIC into the field-replaceable radio modules for the RT1100 and RT1700 Radio Terminals. (Appendix A lists radio and scanner modules.) Norand also preinstalls the NIC into the RT5900 Radio Terminal; Norand or other qualified service personnel must replace the NIC.

ISA (Proxim 2.4 GHz)

The ISA wireless NIC is a high-performance adapter for PC AT-bus or PC-compatible computers. The NIC supports ODI and NDIS drivers. Norand provides NIC software on diskette. For proper network communications, you must load the software into the computer and configure it according to your site's requirements.

The ISA NIC consists of a standard network adapter card that plugs into the system unit's ISA bus slot (8 bit or 16 bit), and an antenna unit that connects to the card through a connector.

For best performance the antenna unit sits on the top of the computer or desk. Figure 5-4 shows a computer with an installed ISA NIC; the antenna unit is on top of the system unit. Norand or certified providers can provide additional placement information through a formal site survey.



1. Antenna unit
2. Connector

Figure 5-4
ISA Wireless NIC

PC-Compatible Computers

Portable, hand-held PC-compatible computers by Norand include members of the PEN*KEY family. PEN*KEY computers communicate with 6710 Access Points as part of a wireless network infrastructure (except for PEN*KEY computers in a peer-to-peer or ad hoc configuration). Wireless NICs and software drivers installed in the computers make them appear to be nodes physically connected to the wired Ethernet medium.

PEN*KEY computers are designed for job-specific applications such as forms-based computing. They offer touch, pen, and keyboard data entry, and can capture signatures for transaction verification. The following pages briefly describe PEN*KEY models for the open system. Contact a Norand representative to find out which model would work best in your environment.

PEN*KEY 6100 Computer

The PEN*KEY 6100 Computer (Figure 5-5) is a Windows- and DOS-based computer. For local area communications, the PEN*KEY 6100 uses the Proxim 2.4 GHz radio option.

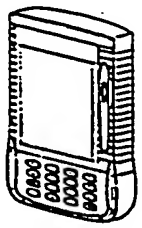


Figure 5-5
PEN*KEY 6100 Computer

The PEN*KEY 6100 Computer's display and keyboard enhance portable computing. The 4.95" diagonal display is touch-activated; a screen stylus is available for signature capture. The keyboard has 16 numeric, tactile keys. You use the keyboard and optional scanner (integrated standard, long-range laser, tethered wand, CCD, or laser) to enter bar code and numeric data.

Two Type II card slots and one Type III slot are other options for the PEN*KEY 6100. More information about these and other options is in the *PEN*KEY 6100 Computer User's Guide (NPN: 961-028-085)*.

PEN*KEY 6400 Computer

The PEN*KEY 6400 Computer (Figure 5-6) is a DOS-based computer that offers wireless access to applications requiring realtime, local-area communications for Ethernet-capable systems. The PEN*KEY 6400 also offers enhanced battery capacity and management. Its lithium ion battery pack incorporates a processor-based logic circuit that performs battery management and charging control.

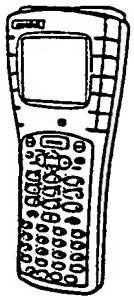


Figure 5-6
PEN*KEY 6400 Computer

The PEN*KEY 6400 Computer's display and keyboard enhance portable computing. The display size is 2.4" (diagonal). The keyboard has 41 or 51 alphanumeric, tactile keys. You use the keyboards and optional scanner (integrated standard, long-range laser, integrated CCD, tethered wand, CCD, or laser) to enter bar code and numeric data.

Two Type II card slots and one Type III slot are other options for the PEN*KEY 6400. More information about these and other options is in the *PEN*KEY 6400 Computer User's Guide (NPN: 961-028-093)*.

PEN*KEY 6600 Computer

Users enter information on the PEN*KEY 6600 Computer (Figure 5-7) through a standard inductive pen or an optional touch-activated screen. Information can also be entered through an external PS/2 style keyboard, which allows customized software solutions to run with off-the-shelf office automation software packages.

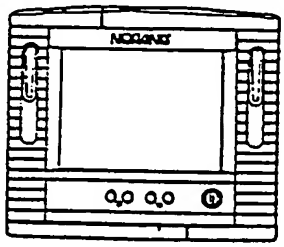


Figure 5-7
PEN*KEY 6600 Computer

The PEN*KEY 6600 is Windows- and DOS-based. Its display has a power-managed backlight and an automatic temperature compensated contrast. Other features include a 486 DX2 50 MHz microprocessor, 2 to 8 MB FLASH expansion modules, and 4, 8, or 16 MB optional internal DRAM expansion modules. Optional modem and scanning options include an RJ11 connection for modems and integrated scanning (both standard and long-range).

The PEN*KEY 6600 can accommodate two Type II card slots and one Type III slot. More information about these and other options is in the *PEN*KEY 6600 Computer User's Guide (NPN: 961-028-084)*.

Development Environments

Because PEN*KEY computers have standard DOS or Microsoft Windows operating systems (or both), you can employ a range of tools to develop custom applications. Their PC architecture opens them to any standard interface.

Most PEN*KEY computers support software developed specifically for pen-based systems. PEN*KEY computers also provide application support for Microsoft C, C++, Visual Basic, and other DOS- and Windows-compatible languages. A major benefit of this open system approach is that you can purchase development tools and software from several vendors, including Norand. This lets you select the equipment and software tools that apply to your development.

Software developer tool kits are available for PEN*KEY computers. The file complement of the tool kits differs among software releases. Tool kits contain DOS or Windows resources (or both) for configuration, power management, communications, and peripherals.

Development information is in these references:

- *PEN*KEY Model 6100 Computer Programmer's Reference Guide (NPN: 977-054-001)*
- *PEN*KEY Model 6200/6300 Computer Programmer's Reference Guide (NPN: 977-054-003)*
- *PEN*KEY Model 6600 Computer Programmer's Reference Guide (NPN: 977-054-002)*

ODI and NDIS Drivers

The wireless infrastructure complies with protocol stacks that support ODI and NDIS driver specifications. Each driver supports multiple standard protocol stacks, which reside above the driver.

EXAMPLE:

A PC-compatible computer (such as a PEN*KEY 6100) could have a Proxim 2.4 GHz wireless NIC running the ODI driver with the TCP/IP stack by FTP Software, Inc., and the IPX/SPX stack by Novell. The PEN*KEY computer would communicate with a 6710 Access Point, which bridges the PEN*KEY computer's Ethernet packets onto the wired Ethernet medium. The PEN*KEY computer operates as if it was a node physically connected to the local wired Ethernet segment.

Section 6

Host Connectivity

About This Section

This section provides an overview of NORAND® host connectivity devices and terminal emulation stations. It also describes the terminal emulation protocol stack.

Host Connectivity Devices

Norand provides high-performance gateway products and terminal emulation stations optimized for use over the wireless medium. The gateways connect to or reside within host computer systems and replace existing multiterminal controllers. Gateways provide direct connections to the Ethernet medium. They support network and transport connections over the wireless infrastructure through the 6710 Access Point to the terminal emulation stations.

NORAND host connectivity devices are the RC4030E Gateway, Wireless Network Access Server, and 6950 Enterprise Gateway Server. The following pages describe these products.

RC4030E Gateway

The RCB4030E Gateway (Figure 6-1) is a protocol-dependent device. It operates as a gateway (protocol translator) between the host computer and the terminal emulation stations on the wireless network.

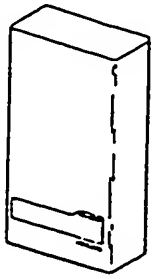


Figure 6-1
RC4030E Gateway

The RC4030E Gateway picks up — via the 6710 Access Point — NORAND packets from terminal emulation stations. The gateway translates the packets into the appropriate host protocol and sends the data to the host through its host port.

You can configure an RC4030E Gateway as one of these controllers:

- IBM 3174 or 3274 Cluster Controller. To the host, the wireless station configured for 3270 terminal emulation appears to be an IBM 3278 Model 2 terminal.
- IBM 5294 or 5394 Control Unit. To the host, the wireless station configured for 5250 terminal emulation appears to be an IBM 5291 Display Station.
- Asynchronous. To the host, the wireless station configured for NORAND Native emulation appears to be an ASCII terminal.

The *RC4030E Gateway User's Guide (NPN: 961-047-087)* describes how to set the controller type and other gateway configuration options. These publications provide more information on terminal emulation:

- *3270 Terminal Emulation Programmer's Reference Guide (NPN: 977-047-040)*
- *5250 Terminal Emulation Programmer's Reference Guide (NPN: 977-047-039)*
- *Native Terminal Emulation Asynchronous Programmer's Reference Guide (NPN: 977-047-038)*

6910 Integrated Gateway/Access Point

The 6910 Integrated Gateway/Access Point (Figure 6-2) combines the functionality of the RC4030E Gateway and 6710 Access Point to support the NORAND Native communications type for small installations.

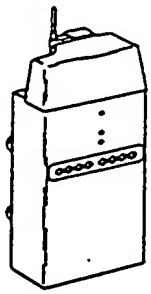


Figure 6-2
6910 Integrated Gateway/Access Point

As an optional wired bridge, the gateway/access point bridges frames between the wired Ethernet LAN and the wireless stations on the radio network. An optional gateway/access point function is to serve as the connection point for several types of wireless stations, which include NORAND terminal emulation stations and PC-compatible computers.

When configured with host options, the gateway/access point picks up data frames from the terminal emulation stations. It translates the frames into the appropriate host protocol and sends the data to the host through the gateway/access point's diagnostic port.

The *6910 Integrated Gateway/Access Point User's Guide (NPN: 961-047-095)* describes how to set host and other gateway/access point configuration options. More information about the NORAND Native communications type is in the *Native Terminal Emulation Asynchronous Programmer's Reference Guide (NPN: 977-047-038)*.

Wireless Network Access Server

The Wireless Network Access Server (WNAS) is a *software* component that provides TELNET capability for VT220 terminal emulation. WNAS is installed and configured on hosts with specified operating systems. When it is infeasible to install WNAS onto the host, the 6950 Enterprise Gateway Server provides similar functionality.

Versions of WNAS support the computer operating systems listed in Table 6-1.

Table 6-1
Operating Systems WNAS Supports

Operating System	Operating System Version
SCO UNIX	4.2 or later
IBM AIX	3.2 or later
HP UX (Series 800)	9.04 or later
Sun Solaris	2.4 or later
IBM OS/2	2.1 or later

WNAS uses the client-server concept: The host computer is the server, and the terminal emulation stations are the clients. This lets software developers write applications for the wireless stations, which are independent of the host computer operating system.

WNAS supports these interfaces:

- VT220 terminal emulation (TELNET) for situations requiring direct connection into existing applications. To the host, the wireless station configured for VT220 terminal emulation appears to be a VT220 terminal.
- NORAND Application Development Kit (ADK) for applications requiring client functionality at the terminal emulation level.

These publications provide more information: *VT220/ANSI Terminal Emulation Programmer's Guide (NPN: 977-047-037)* and *Application Developer's Kit Reference Manual (NPN: 961-051-001)*. The *Wireless Network Access Server User's Guide (NPN: 961-051-006)* describes the WNAS product.

6950 Enterprise Gateway Server

Another host connectivity option is the 6950 Enterprise Gateway Server (Figure 6-3). The gateway server communicates —via the 6710 Access Point — frames from terminal emulation stations running VT220 terminal emulation. The gateway server then translates the packets into a standard TELNET session, and puts the data back onto the Ethernet LAN with the host running TCP/IP.

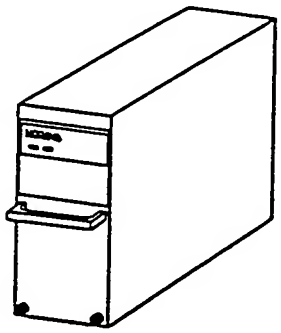


Figure 6-3
6950 Enterprise Gateway Server

When the gateway server is booted it establishes a connection to the terminal emulation station based on the data it gets from system setup files. As each wireless station powers on, it establishes a terminal session with the host. The *6950 Enterprise Gateway Server User's Guide* (*NPN: 961-047-091*) has more information about gateway server operation and setup.

Terminal Emulation Stations

Terminal emulation stations for the open system include the PEN*KEY® 6400 Computer and radio terminals in these series: RT1100, RT1700, and RT5900.

PEN*KEY 6400 Computer

PEN*KEY 6400 Computers can operate as a wireless station running 3270, 5250, VT220, or NORAND Native terminal emulation. More information about how to set up, maintain, and operate the PEN*KEY computer is in the *PEN*KEY 6400 Computer User's Guide (NPN: 961-028-093)*.

RT1100 Radio Terminal

RT1100 Radio Terminals (Figure 6-4) are a series of lightweight "pocket RF" radio terminals designed primarily for retail use. The radio terminal is 6.875" long x 2.625" wide x 1.375" deep and has an elastomer, 47-key keyboard with alphabetic and numeric keys.

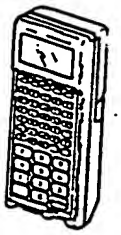


Figure 6-4
RT1100 Radio Terminal

The radio terminal's liquid crystal display has 4, 6, 8, or 9 lines by 12 or 16 characters. (Sizes are adjusted by the user.) The display also has a backlight and full bit-mapped graphics capability.

The radio terminal's scanner and radio modules are interchangeable. You can upgrade the radio terminal by changing its module to accommodate changing application needs or new radio technologies. More information about how to set up, operate, and maintain the radio terminal is in the *1100 Series User's Guide (NPN: 961-047-069)*.

RT1700 Radio Terminal

Radio terminals in the RT1700 Series (Figure 6-5) operate in industrial and retail environments. The radio terminals have an optional vehicle mount, which makes them useful for "pick and run" applications.

The radio terminal is 9.75" long x 2.625" wide x 1.375" deep. It has a elastomer 57- or 37- key keyboard with alphabetic and numeric keys, plus a scanner key. Its black-on-white liquid crystal display has 8, 10, 16, or 21 lines x 16, 21, or 26 characters. (Sizes are adjusted by the user.) The display also has a backlight and full bit-mapped graphics capability.

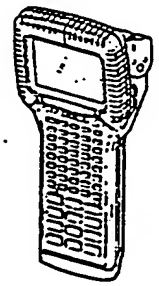


Figure 6-5
RT1700 Radio Terminal

The radio terminal's scanner and radio modules are interchangeable. You can upgrade the radio terminal by changing its module to accommodate changing application needs or new radio technologies. More information about how to set up, operate, and maintain the radio terminal is in the *1700 Radio Terminal User's Guide (NPN: 961-047-068)*.

RT5900 Mobile Mount Radio Terminal

Mobile mount radio terminals in the RT5900 Series (Figure 6-6) meet NEMA 3 standards for ruggedness and durability in harsh environments. The radio terminal can be removed from its mounting bracket and mounted onto a forklift. The radio terminal can also be used on a desktop as a wireless radio terminal for manufacturing processing.

RT5900 Radio Terminals have a tactile 57-key keyboard with alphabetic and numeric keys. The radio terminal's liquid crystal display provides graphics capabilities and sizes from 8 lines by 40 characters up to 25 lines by 80 characters. Sizes are adjusted by the user.

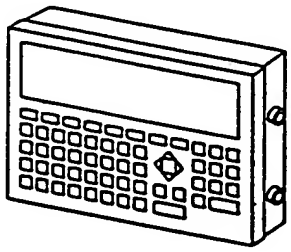


Figure 6-6
RT5900 Mobile Mount Radio Terminal

More information about how to set up, operate, and maintain the radio terminal is in the *RT5980 Radio Terminal User's Guide (NPN: 961-047-092)*.

Host Protocol Support

Terminal emulation stations support IBM 3270 SNA/SDLC, IBM 5250 SNA/SDLC, and NORAND Native terminal emulations through the RC4030E Gateway, and NORAND Native through the 6910 Integrated Gateway/Access Server.

Terminal emulation stations support VT220 terminal emulation through WNAS software or the 6950 Enterprise Gateway Server. WNAS and the gateway server support connectivity to networks with TCP/IP protocols.

Application Integration Tools

You can use a range of tools to develop custom applications for PEN*KEY 6400 Computers and radio terminals. Tools include Microsoft C and the ADK C libraries by Norand.

Terminal Emulation Protocol Stack

The terminal emulation protocol stack provides efficient data exchange over the wireless infrastructure. When compared to off-the-shelf emulations written for standard PCs, the protocol stack promotes large wireless station populations with low response times and improved battery management. The protocol stack also enables terminal emulations to coexist with industry-standard protocols operating over the wireless infrastructure. Figure 6-7 shows the terminal emulation protocol stack.

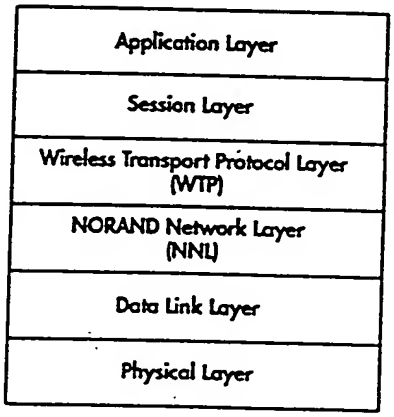


Figure 6-7
Terminal Emulation Protocol Stack

The NNL protocol uses an Ethernet protocol type of hexadecimal 875B. Data frames (such as a frame carrying data from a NORAND RT1700 Radio Terminal to the RC4030E Gateway via a 6710 Access Point) are carried as NNL-type frames. NNL frames are usually not sent to the multicast address; instead they are sent to the MAC (physical) address of the actual network device they are enroute to.

EXAMPLE 1: A data frame from an RT1700 Radio Terminal (with a Proxim 2.4 GHz radio module) to an RC4030E Gateway would have a source address of 00:20:A6:xx:xx:xx (the Ethernet vendor address for Proxim) and a destination address of 00:C0:B2:xx:xx:xx (the Ethernet vendor address for Norand).

EXAMPLE 2: A data frame from an RT1700 Radio Terminal (with a Proxim 2.4 GHz radio module) to a 6950 Enterprise Gateway Server would have a source address of 00:20:A6:xx:xx:xx (Ethernet vendor address for Proxim) and a destination address of 00:00:0C:xx:xx:xx or 00:80:0F:xx:xx:xx (the vendor address for Western Digital or SMC, the manufacturers of the Ethernet adapter card for the gateway server).

Dashed lines in Figure 6-8 show data flow through the terminal emulation protocol stack. The terminal emulation station is set up for 5250 SNA/SDLC, 3270 SNA/SDLC, or NORAND Native terminal emulation. The host connectivity device for these types of terminal emulation is the RC4030E Gateway.

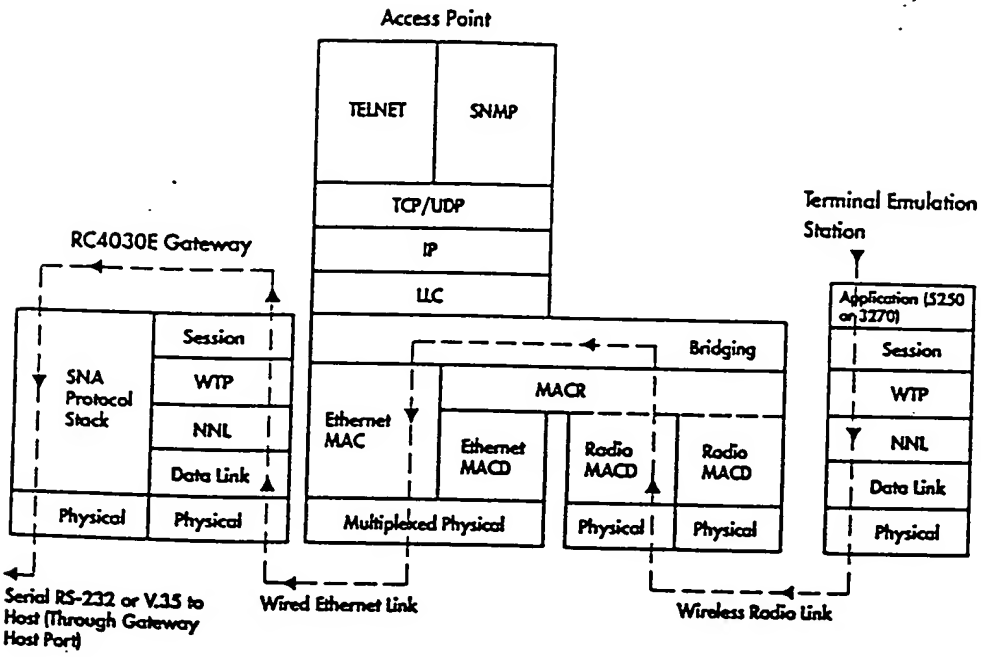


Figure 6-8
Data Flow Through Terminal Emulation Protocol Stack (RC4030E Gateway)

Figure 6-9 shows another example of data flow through the terminal emulation protocol stack. In this figure, the terminal emulation station is set up for VT220 terminal emulation. In this example, the host connectivity device for VT220 terminal emulation is the 6950 Enterprise Gateway Server. Note that the gateway server converts the terminal emulation protocol stack into a TELNET session to the host.

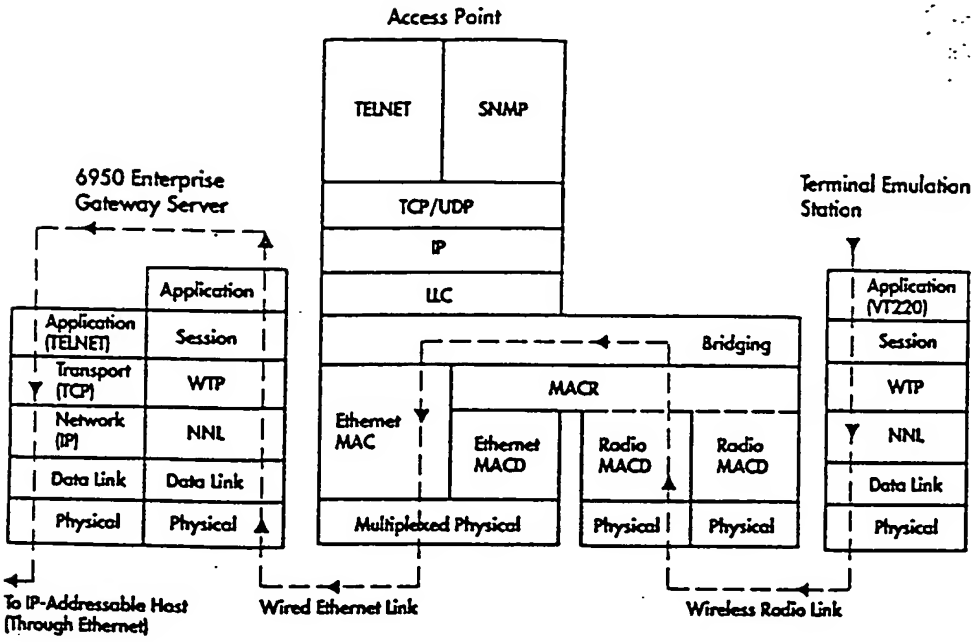


Figure 6-9
Data Flow Through Terminal Emulation Protocol Stack (6950 Enterprise Gateway Server)

Section 7

Wireless Access Points

About This Section

An access point with the 900 MHz or UHF radio option can be a wireless access point, which provides a range of connectivity solutions. This section describes wireless access points and the solutions they provide.

Operation

A *wireless access point* is an access point that does not physically connect to the Ethernet medium. The wireless access point provides a wireless store-and-forward operation (a *hop*) with each frame transmitted twice over the wireless media to reach its destination. Because frames are transmitted twice, the amount of wireless traffic over the radio network doubles.

In general, the throughput of a wireless access point has about half the effective bandwidth of a wired bridge, because all frames received on the radio channel must be forwarded on the same channel. Therefore, using a wireless access point exchanges performance for ease of installation.

Figure 7-1 shows how a wired bridge overlaps coverage with a wireless access point. Note how the coverage areas of the devices overlap more than the areas of wired bridges.

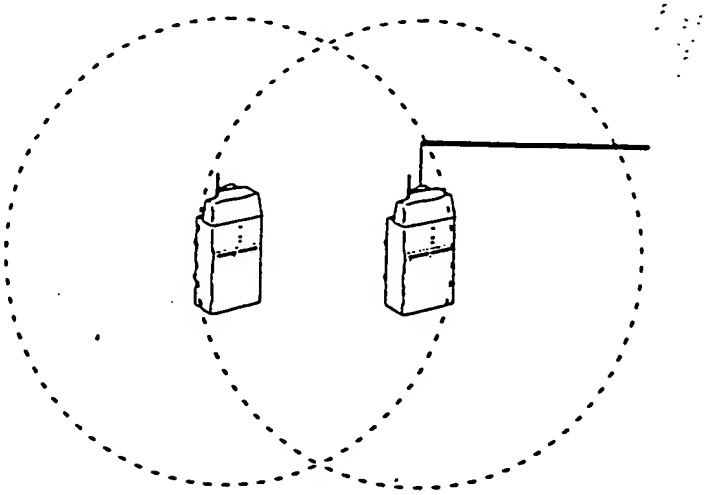


Figure 7-1
Overlapping Coverage of Wired Bridge and Wireless Access Point

When wired and wireless access points overlap coverage, wireless stations will automatically switch between them. Wireless stations base their choice on which device offers the best path. They choose a wired bridge over a wireless access point, for example.

For best coverage, wireless access points are usually mounted high on a wall or post, or on the ceiling, to do the following:

- Expand the coverage area
- Reduce the amount of cable
- Cover fringe areas
- Provide redundancy
- Meet temporary coverage needs

Expanding the Coverage Area

Multiple wireless access points can expand the coverage area. However, each additional wireless access point introduces an additional wireless hop and a corresponding reduction in throughput or an increase in response time. Norand does not recommend extensive use of wireless hops in performance-critical areas. Generally, a single wireless hop will not result in a discernable reduction in performance, unless extensive data transfers are required.

Figure 7-2 shows multiple access points and coverage areas. In the figure the wireless station is associating with wireless access point A. A forwards frames to wireless access point B, which forwards them to access point C (a bridge wired to the Ethernet medium). A network with this many hops would have some performance limitations.

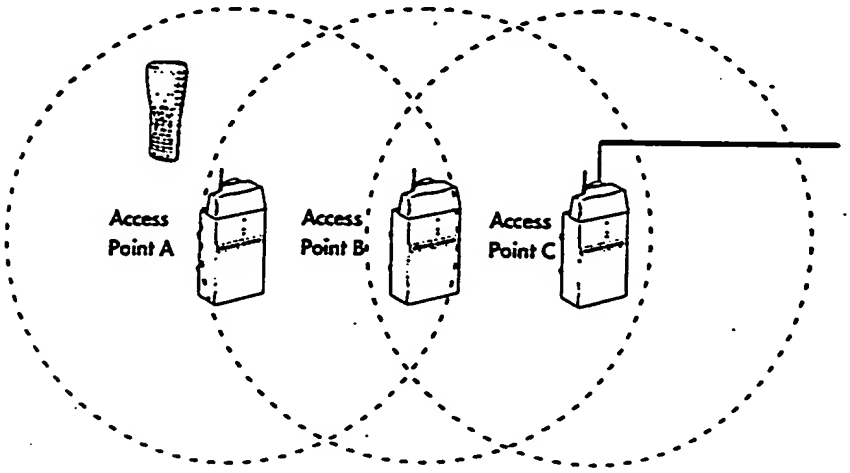


Figure 7-2
Expanding the Coverage Area Through Wireless Access Points

Reducing the Amount of Cable

Wireless access points can reduce the amount of cable needed. The design in Figure 7-3 shows how four wireless access points (in black) reduce the amount of cabling in a warehouse.

▶ NOTE: *This symbol represents an access point:* 

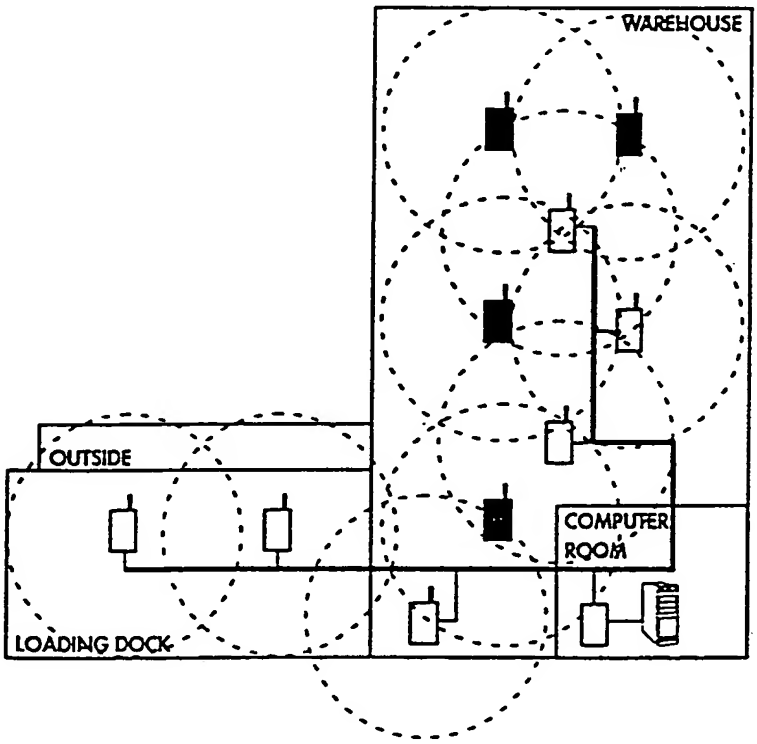


Figure 7-3
Reducing the Amount of Cable Through Wireless Access Points

This example has several advantages:

- It needs more wireless access points, but they are not wired to a physical medium.
- It does not need a repeater.
- It reduces the cable length.
- It results in only one hop from any area.

Wireless access points are not located in the loading dock because the traffic there is heavy and top performance is required.

Covering Fringe Areas

A wireless access point can provide coverage in fringe areas. For example, if an area has marginal coverage, you could mount one or two wireless access points in the area. No cabling would be required.

Figure 7-4 shows how two additional wireless access points (in black) fill in fringe areas on the outside of the loading dock. Heavy dashed circles show their coverage areas.

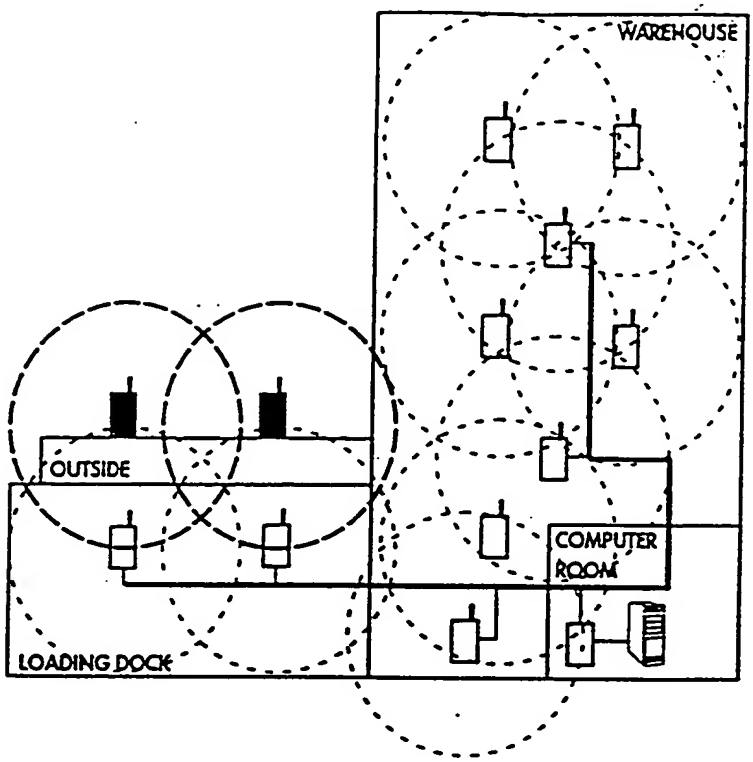


Figure 7-4
Covering Fringe Areas Through Wireless Access Points

Providing Redundancy

Another benefit of a wireless access point is *redundancy*. If properly designed, an installation with wireless access points can ensure that no single device failure or single cable cut can stop service. You can reduce costs by providing redundancy only in selected areas. A site planning to install one or more wireless access points should coordinate the effort with their Norand representative.

Figure 7-5 shows an example of how an access point (in black) wired to 10BASE2 can become a wireless access point and continue coverage if it becomes disconnected from the physical medium.

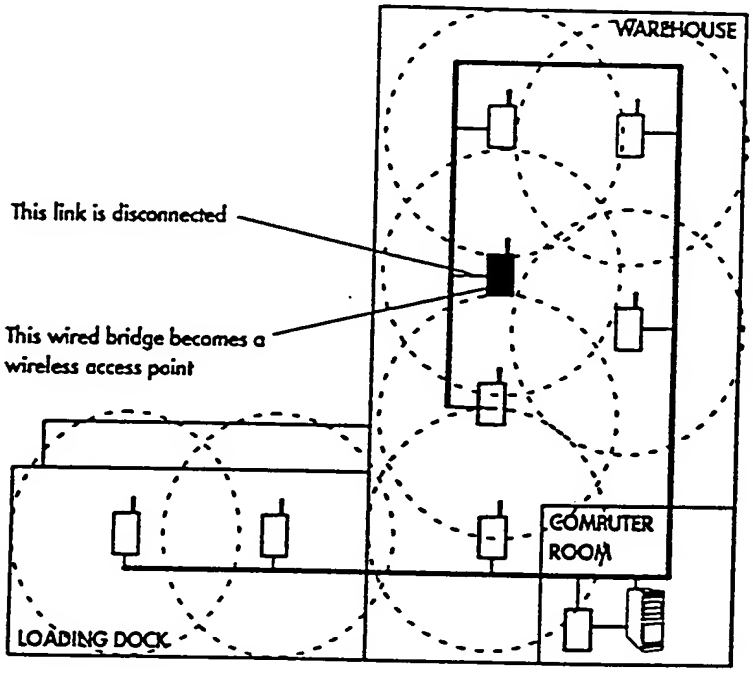


Figure 7-5
Warehouse With Wireless Access Point on 10BASE2

Figure 7-6 shows an example of how an access point wired to 10BASE-T can become a wireless access point and continue coverage if its link to the hub is cut.

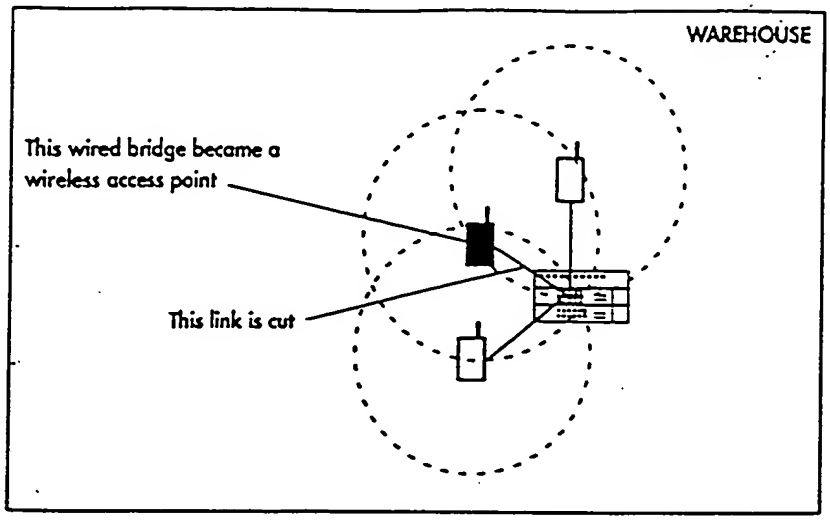


Figure 7-6
Warehouse With Wireless Access Point on 10BASE-T

Meeting Temporary Coverage Needs

Wireless access points can handle a temporary need without the effort or expense of additional cabling. For example, the wireless access point shown in black in Figure 7-7 can provide coverage in a temporary addition.

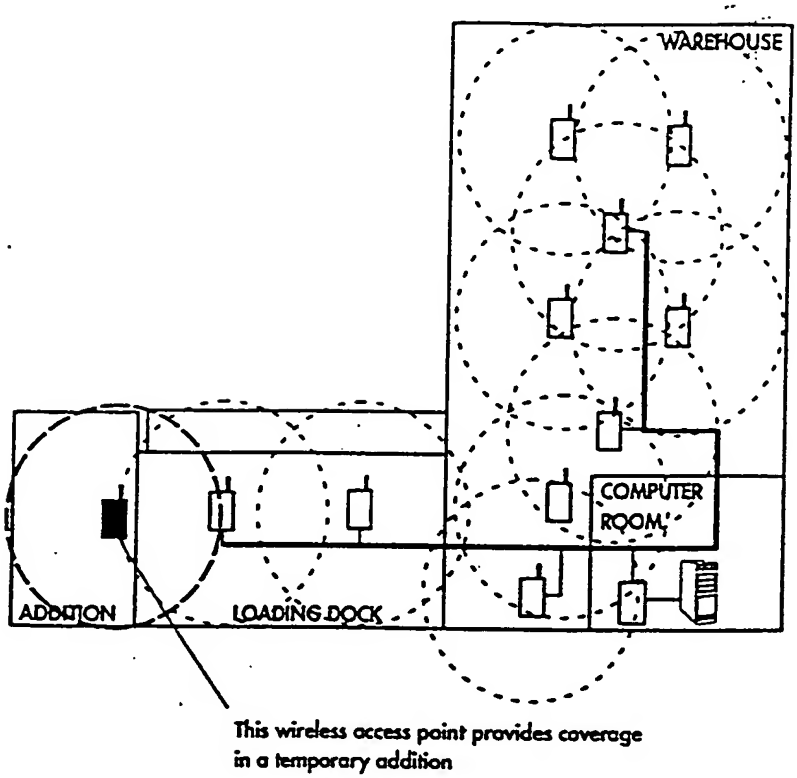


Figure 7-7
Wireless Access Point Meeting Temporary Need

One of the advantages of wireless access points is the ease with which you can install them. To improve coverage in a dead spot, you could temporarily install a wireless access point to see if it helps. If it solves the coverage problem but the performance is unacceptable, you could wire to the physical medium.

If the coverage at your site is satisfactory but the performance of the wireless access points needs to improve, you could connect them to the physical medium. You could also use a wireless access point to experiment with coverage by moving the bridge around, before running cables.

Section 8

Installation

About This Section

Each network installation is unique because each site has different computing equipment and requirements. In general, an installation should emphasize modular cabling systems and a network topology you can easily configure, maintain, and update to meet changing application needs.

Before you install the wireless infrastructure you should consider these strategies:

- Conducting a site survey
- Selecting the Ethernet medium
- Extending the network
- Using existing media
- Using routers

This section has useful overviews of each strategy. The overviews help you design a flexible, open wireless LAN with NORAND® wireless infrastructure components and off-the-shelf network devices such as bridges, routers, and repeaters.

This section also shows how wireless infrastructure components and host connectivity devices connect to Ethernet media. Examples of some simple warehouse and retail installations follow the illustrations.

Conducting a Site Survey

Norand strongly recommends that you conduct a site survey to determine the network solutions for your site. A site survey (such as those conducted by Norand or certified providers) requires special equipment and training. Because it helps you build a system capable of supporting your traffic requirements, the site survey can improve the performance of the open wireless LAN.

A site survey determines the optimum number and placement of 6710 Access Points to provide reliable wireless coverage of your facility. Many factors affect coverage, including the floor plan, building construction, usage needs, and materials or equipment stored or used within the environment.

This section does not provide the detailed information you may need if you have or will have a large network. In this case, you should contact your Norand representative or a certified provider for more information.

Selecting the Ethernet Medium

The following pages provide basic facts about 10BASE2, 10BASE-T, and 10BASE5. For more specific information about these cable types and their electrical and mechanical requirements, refer to the ANSI/IEEE 802.3 standard.

▶ NOTE: *Norand recommends that sites use only ANSI/IEEE 802.3 standard media and equipment. ANSI/IEEE standards promote configuration guidelines with performance expectations. Vendors should be able to provide the ANSI/IEEE standards and specifications that apply to their products.*

10BASE2

10BASE2 or "thinnet" is a commonly-used type of Ethernet medium. It is popular for several reasons including the following:

- It is highly flexible, which makes it easy to work with.
- It is less susceptible to electromagnetic interference than 10BASE-T.
- It does not require hubs (as 10BASE-T does). This lowers the cost of an attachment to the network.

10BASE2 has some disadvantages. One is that the length of each cable segment is limited to about 607 feet (185 meters) or one-tenth of a mile. Repeaters and bridges, however, can extend the length limit. Repeaters and bridges are covered later in this section.

Cable Characteristics

Cables approved by ANSI/IEEE for use with 802.3 10BASE2 Ethernet are:

- 802.3 10BASE2: 50 ohms, stranded tinned core
- RG58 A/U: 50 ohms, stranded tinned core
- RG58 C/U: 50 ohms, stranded tinned core

RG58 and RG58 U coaxial cables have solid center cores. They physically resemble RG58 A/U cable but do not comply with ANSI/IEEE Std 802.3 for 10BASE2. Therefore, RG58 and RG58 U cables should not be used.

▶ NOTE: *When obtaining 10BASE2 coaxial cable, request that it be certified for use with ANSI/IEEE Std 802.3 for 10BASE2. Cheap substitutions are not reliable.*

T-connectors

The 6710 Access Point, RC4030E Gateway, and 6950 Enterprise Gateway Server have industry-standard BNC ports for quick, easy connection to 10BASE2. A T-connector attaches to the BNC port and to the 10BASE2 cable.

T-connectors are available in three impedances: 50 ohms, 75 ohms, and 93 ohms. The difference among them is the diameter of the center pin. Mating T-connectors with different impedances can damage one or both connectors or result in an unreliable connection.

The 10BASE2 RG58 A/U or C/U coaxial cable is 50 ohms. Therefore, you must use 50-ohm T-connectors to connect the fixed-end devices to 10BASE2. A T-connector cover insulates the T-connector from electrostatic discharge when it is not in use.

Cable Terminators

T-connectors on fixed-end devices at each end of the coaxial cable must be fitted with 50-ohm cable terminators, which maintain the impedance of the network. The network will function properly only if each end has an attached cable terminator. The terminator has a BNC coaxial connector.

Many repeaters (and some bridges and routers) have built-in terminators. Bridges and routers often have a switch that enables or disables the terminator, because they are not always at the ends of segments. If the last repeater or bridge on the segment has a built-in terminator, you should not use an external one. The network will not operate properly if more than two terminators are installed on a segment.

Segment Rules

A 10BASE2 cable segment is the length of cable between cable terminators. According to ANSI/IEEE standard specifications the following rules apply:

- The length of each segment can be no longer than about 607 feet (185 meters).
- 30 or fewer network devices can be attached to a segment. Each repeater counts as a network device.
- Cable runs between 10BASE2-connected devices must be 1.64 feet (0.5 meters).

These rules ensure that signal losses are within acceptable limits. They also limit the amount of signal attenuation and distortion on a segment. The standard 185-meter length lets you use 10BASE2 Ethernet components that conform to the ANSI/IEEE standard.

Topology

10BASE2 networks form a bus topology. The coaxial cable forms a line that connects each network device. T-connectors daisy-chain the 10BASE2 cable from one network device to the next, with cable terminators at the ends of each segment. Repeaters join 10BASE2 segments end-to-end; they can also be installed in the middle of a segment. Bridges and routers can join segments in the middle to form X- or T-shaped networks.

Summary of 10BASE2

Table 8-1 summarizes 10BASE2 characteristics. Refer to ANSI/IEEE 802.3 standard specifications for detailed information about design and installation rules.

Table 8-1
10BASE2 Characteristics

Feature	Description
ANSI/IEEE standard	802.3 10BASE2
Data rate	10 Mbps
Topology	Bus (linear)
Maximum cable segment length (without repeaters)	607 feet (185 meters)
Maximum network length (without bridges)	3034 feet (925 meters)
Maximum number of segments	5 (only 3 can be populated)
Maximum number of repeaters	4
Maximum number of network devices per segment	30
Maximum number of network devices per network	1024
Minimum distance between network devices	1.64 feet (.5 meters)
Cable type	RG58 A/U, 0.2 inches diameter, single shielded

10BASE-T

10BASE-T is a popular Ethernet medium. Some reasons are:

- It is easy to install.
- Its star-wired topology makes it easy to troubleshoot because problems can be isolated to a cable or hub (also called a concentrator or multiport repeater).
- A cable break from the hub to a network device disables only the network device at the end of the cable.
- You can easily expand the network by connecting several hubs to each other. This topology is called a modified star configuration, and creates a geographically dispersed network.
- Intelligent hubs provide maintenance, monitoring, and management capabilities unavailable for most other cabling schemes.

The star-wired topology has some disadvantages. One is that additional cabling and connection equipment (such as hubs) are required. Another disadvantage is that a cable break between two connected hubs can bring down many network devices.

Because 10BASE-T uses unshielded cable, problems may develop in electrically-noisy environments such as heavy industrial areas. If this happens the 10BASE-T cables can be shortened, relocated away from the noise source, put in metallic conduits, or shielded. However, the best solution may be to change to another form of Ethernet.

Cable Characteristics

10BASE-T uses unshielded twisted pair (UTP) cable. Sites should use only data grade UTP cable that is verified UTP Category 3, 4, or 5 and installed per IEA/TIA 568–569.

10BASE-T cable is often installed using various telephone wiring methods. The methods followed to form the connection from the device to the hub vary with local practices. However, the connection provided at the fixed-end device's location should always be an RJ45 modular jack.

▶ NOTE: *The cable from the network jack to the network device must be a twisted-pair cable. Avoid using the nontwisted cables often used for telephones.*

The length limit from the network device to the hub is just 328 feet (100 meters). There may already be close to that in the wall extending from the jack back to the hub. So, it is best to keep the cable from the network jack to the network device as short as reasonably possible.

RJ45 Plug

The standard connector for 10BASE-T is an RJ45 modular plug. The plug physically resembles the RJ11 modular plug used to plug most telephones into the wall. The 6710 Access Point, RC4030E Gateway, and 6950 Enterprise Gateway Server have standard RJ45 ports for connection to 10BASE-T.

Connecting to Hubs

A hub is a repeater. On a 10BASE-T network, hubs are multiport repeaters.

Topology

10BASE-T networks form a star topology. Each network device has a separate cable that extends from a central hub to the network device, with the hub at the "center" of the star. Hubs can connect to each other to extend the network beyond the number of network devices that a single hub supports. Multiple hubs connected together form a modified star topology.

Summary of 10BASE-T

Table 8-2 summarizes 10BASE-T characteristics. Refer to ANSI/IEEE 802.3 standard specifications for detailed information about design and installation rules for 10BASE-T.

Table 8-2
10BASE-T Characteristics

Feature	Description
ANSI/IEEE standard	802.3 10BASE-T
Data rate	10 Mbps per second
Topology	Star
Maximum number of segments	5

Table 8-2 (Continued)
10BASE-T Characteristics

Feature	Description
Maximum number of repeaters	4
Maximum cable length between network device and hub	328 feet (100 meters)
Maximum number of network devices/segment	512
Minimum space between network devices	10 feet (.5 meters)
Connector type	RJ45
Twisted pair cable	

10BASE5

10BASE5 is also called "thicknet." Generally, it is only used in specific applications because:

- It uses RG8 coaxial cable, which is heavy and rigid.
- 10BASE5 transceivers (also called media attachment units, or MAUs) tend to be physically heavy.
- 10BASE5 N-connectors and vampire taps are large and difficult to install under field conditions.

10BASE5 does have some advantages. One is that segments can be up to about 1640 feet (500 meters). Also, the cable flow can be easily followed when troubleshooting. And 10BASE5 does not require hubs as 10BASE-T does.

10BASE5 is most often used to cover long distances as a backbone cable. A "backbone" is the main cable installed in a building to provide wired connectivity to separate areas. Backbone cables are usually not designed for direct system access.

▶ NOTE: *Refer to ANSI/EEE 802.3 standard specifications for detailed information about design and installation rules for 10BASE5.*

Extending the Network

Following are standard segment length limits:

- 10BASE2 is 607 feet (185 meters)
- 10BASE-T is 325 feet (100 meters)

The following pages describe how repeaters and bridges can extend these standard segment lengths.

Repeaters

A repeater is a local network device that extends the LAN length and topology by increasing the distance a LAN can extend and joining two different topologies. Repeaters are simple to install and do not need to be configured.

Operation

Repeaters operate at the Physical layer of the OSI model by receiving data from one segment, amplifying the data, and putting the data out on the next segment. A repeater does not process the data and retransmit it, but simply amplifies it along with any noise on the cable. Because of the noise amplification only a few repeaters can be used within a segment. This requirement establishes the maximum length of an Ethernet segment for the different Ethernet media.

The repeater makes all segments operate as though they were a single segment, or network. This is called a single Ethernet "collision domain." A single collision domain makes it possible for network devices connected to any segment in a system of segments linked by repeaters to hear the same signals, and to operate as a single segment.

A repeater prevents signal loss but extends the network so that signals take longer to travel from one end of the cable to the other. The CSMA/CD protocol depends on all network devices to be able to hear transmissions from other devices within certain timing parameters.

If the segment length is longer than the maximum allowed, a network device's moment of listening may not be long enough for it to hear a transmission from another device. The longer the moment, the longer the network device has to wait before it can transmit. This decreases network effectiveness and is why the Ethernet standard allows only four repeaters on 10BASE2 and 10BASE-T networks.

The moment is long enough for the signal to travel five segments and four repeaters.

Repeater Rules

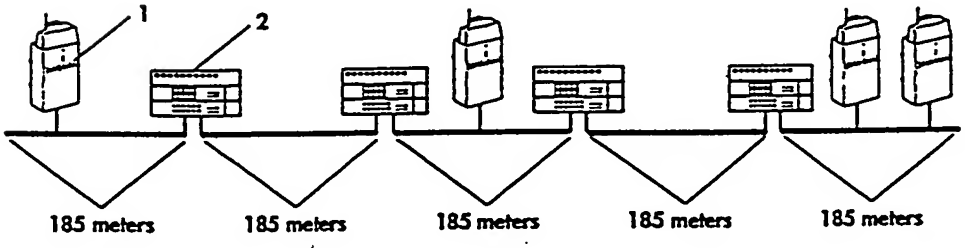
The Ethernet repeater rule is:

> Five segments maximum, interconnected by 4 repeaters (or hubs) in the data transmission path between any two devices in the same collision domain. Three of the segments are populated with nodes, and 2 are interrepeater link segments (for distance). This creates 1 collision domain.

Repeaters on 10BASE2

10BASE2 standards allow a maximum of four repeaters on the network. Four repeaters join five segments. The total network span with five segments is about 3000 feet (925 meters) long. No more than four repeaters can be on the signal path from one network device to any other network device. Figure 8-1 shows a single 10BASE2 network with five segments and four repeaters.

▶ NOTE: *If the repeated network exceeds the Ethernet design limitations (5 segments with 4 repeaters), late collisions and lost packets will occur.*



1. 6710 Access Point
2. Repeater

Figure 8-1
10BASE2 Network With Four Repeaters

Repeaters on 10BASE-T

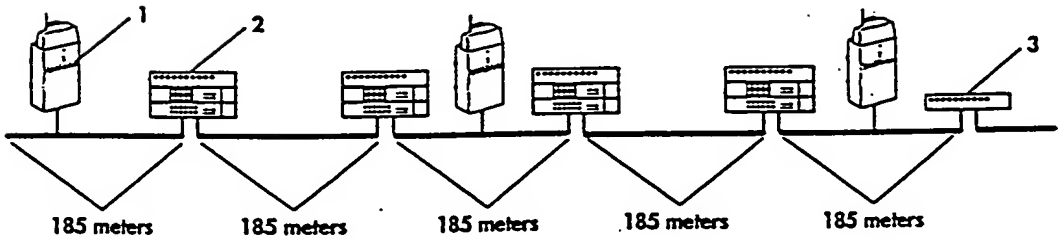
Repeaters with RJ45 (10BASE-T) ports are 10BASE-T hubs. Most hubs support from 8 to 144 ports; however, some vendors offer mini-hubs, which provide 1 to 4 UTP ports for link extension. Each port on the repeater should support the full extent of the ANSI/IEEE specification for 10BASE-T.

Bridges

To go beyond five cable segments for 10BASE2 networks, you need a bridge to receive a packet and then retransmit it on another segment. The number of bridges that can be installed depends on the protocol the bridge is using.

Bridges are intelligent devices that operate at the Data Link layer of the OSI model. They filter packets and provide error checking. Normally, bridges connect segments of similar media and protocol types.

10BASE2 networks can have a maximum of five segments and four repeaters. After the fourth repeater you need to install a bridge to recover the CSMA/CD timing. After the bridge you can install five more cable segments and four repeaters. After the fourth repeater you need to install a second bridge. Figure 8-2 shows a 10BASE2 network with one bridge.



1. 6710 Access Point
2. Repeater
3. Bridge

Figure 8-2
10BASE2 Network With One Bridge

Hybrid Topologies

A larger network span can be created through a hybrid topology, which is created when different topologies are connected.

EXAMPLE: A router can connect 10BASE-T to a bus topology (such as 10BASE2) to form a hybrid topology.

Although 10BASE2 is intended for local use, repeaters can join several segments together to create a larger network span. Similarly, several 10BASE2 segments can be tied into a longer Ethernet backbone.

Some benefits of a hybrid topology are:

- It connects systems that may not be otherwise accessible.
- It connects existing networks so that resources can be shared without installing new cable.

A hybrid topology has some disadvantages.

- It requires bridges and routers to connect the networks.
- More than one person may be required to troubleshoot problems because of different technologies.

Using Existing Media

Some sites already have Ethernet cabling and network devices installed throughout their buildings. The sites may want to use the existing medium for their fixed-end devices, or connect two different topologies. If you are thinking about using the existing cable at your site, you should research answers to the following questions.

- *What type of cable is installed at the site?*

  Sometimes three different types (such as 10BASE5, 10BASE2, or 10BASE-T) are in use. The most important question is which type you will want to connect your fixed-end devices to. The 6710 Access Point and 6950 Enterprise Gateway Server have ports for connection to 10BASE2, 10BASE5, or 10BASE-T. The RC4030E Gateway has ports for connection to 10BASE2 and 10BASE-T.

- *Is the cable physically installed where the devices will be installed?*

  Ethernet cable is usually installed at floor level where most computer equipment is located. So that it can provide maximum radio coverage, the 6710 Access Point is usually installed near the ceiling or in the rafters. Because the RC4030E Gateway has no radio module or antenna, it is usually installed next to the host computer in a computer room.

  Because running connections to access points mounted in the rafters may not be feasible, separate cable can be installed for the access points. Later, the cable with the access points can be bridged to another cable at one point.

- *How heavily utilized are the cable segments the devices will be communicating over?*

  Good response time from wireless stations cannot be expected if fixed-end devices must communicate over an overloaded network. Special instruments can measure network utilization over several days.

Using Routers

Routers are protocol-dependent devices that connect networks and selectively forward packets based on Network layer addresses. For example, a router may forward only IP or IPX packets.

Routers can connect dissimilar protocols and media. They use the Network ID part of the internet address to make the routing decision on each Ethernet packet. Each router exchanges information about the entire network with other routers to maintain current data on the paths through the network. In a network with multiple paths between two devices, a router may select the best path for communications.

Routers forward packets based on path availability, traffic loads, and other factors. If a network device sends two packets to another network device on a network with routers, those packets may take entirely different paths to get from the first network device to the second. Several factors can cause a route from one network device to another to become unavailable.

For example, a network segment may become unavailable if a cable breaks or becomes disconnected, if a repeater or bridge fails, or if a phone line goes down.

Some routers can be configured. For example, inter-access point communications can be enabled by configuring the router to bridge DIX type 0875C packets. NORAND terminal emulation can be enabled by configuring the router to bridge 0875B packets.

Installing Wireless Infrastructure

The following pages describe these installation strategies for the 6710 Access Point as part of the wireless infrastructure:

- Location of the access point
- Mounting options
- Power requirements
- Ethernet connectivity solutions

▶ NOTE: *A person who understands applicable local building codes and is skilled with the tools and equipment used to install FCC Class B electromechanical network devices should install the 6710 Access Point.*

Location

You should locate each 6710 Access Point where it will provide the best performance. The following pages discuss these location strategies:

- Centrally locating the access point
- Using a remote antenna
- Protecting the access point in harsh environments
- Minimizing obstructions
- Resolving other location issues

Centrally Locating the Access Point

The access point should be centrally located within the group of wireless stations. This enables all wireless stations to be within the access point's coverage area. The location for the access point must meet the requirements in Appendix D, "6710 Access Point Specifications."

Using a Remote Antenna

You can use a remote antenna for coverage if you cannot mount an access point in an ideal location. An ideal location in a warehouse, for example, might be near the ceiling at an intersection of aisles. You can mount the antenna near the ceiling in the center of the aisle, but must secure the access point to a column structural support nearby.

NICs that are remote-enabled have a connector for a remote antenna. The antenna attaches to a special connector on the access point's cover either directly or remotely through a coaxial cable. Norand or other qualified personnel must install external antennas.

▶ NOTE: *Only antennas that Norand furnishes may be used with NORAND 6710 Access Points.*

Protecting the Access Point

Norand designed the access point for operation in an enclosed, weather-proof environment. If you need to install an access point in an area that may expose it to excessive heat, humidity, and other harsh elements (such as rain and snow), you can house the access point in an enclosure. The enclosure must meet National Electrical Manufacturing Association (NEMA) standards for environmental protection. Figure 8-3 shows the access point in a NEMA enclosure, which is available from Norand.

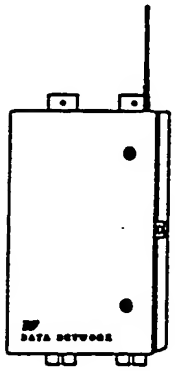


Figure 8-3
NEMA Enclosure

Minimizing Obstructions

You should locate the access point so that a clear line of sight is between the NIC's antenna and the wireless stations. Walls (especially steel reinforced concrete or masonry), floors, office partitions, and other obstructions reduce the effective communications range. You should place the access point where the number of barriers between it and the wireless stations it is communicating with is minimal.

If walls and office partitions prevent you from centrally locating the access point, you should mount the access point as high as possible in another suitable location. In addition, the installed access point must be at least 2 feet from any objects that might negatively affect radio transmissions. Objects include large metal structures and fluorescent lights.

Resolving Other Location Issues

When selecting the best location for each access point keep these other issues in mind:

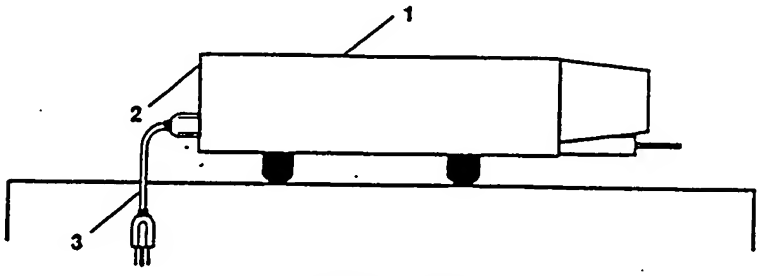
- A person standing on the floor or on a ladder under the access point should be able to easily see the access point's LEDs. The LEDs are useful for troubleshooting and verifying certain operating conditions.
- Leave enough room around each access point so that you can easily connect communication, diagnostic, and power cables to it.
- If possible, another outlet should be available near each access point for LAN test equipment if troubleshooting is necessary.
- The network cabling and access point's power cord must be able to reach the access point after you install it.

Mounting Options

You can mount the access point horizontally on a tabletop, vertically on a wall or post, or on a ceiling. Norand recommends that you mount the access point vertically so that it will be drip-resistant. An access point in any other position must be protected from dripping fluids.

Horizontal Mount

The mounting bracket on the bottom of the access point is not needed for a tabletop installation; you can remove and save the bracket for future use. When the access point is on the tabletop, four rubber feet on the access point's back panel keep it from slipping out of place (Figure 8-4).



1. 6710 Access Point
2. Bottom panel
3. Power cable

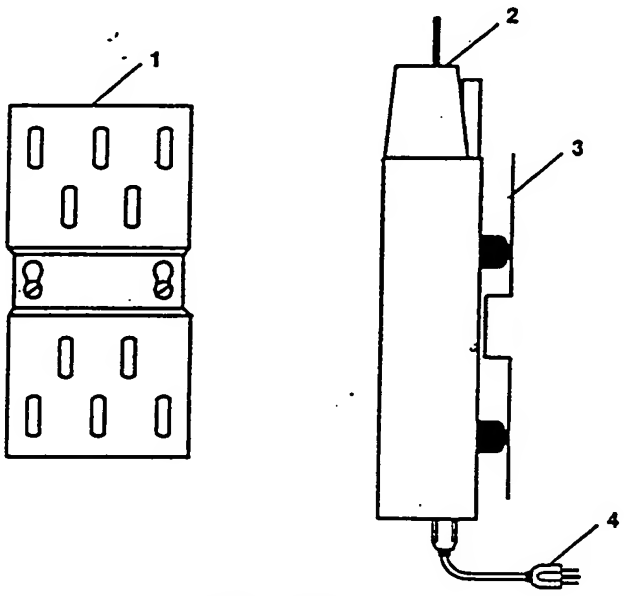
Figure 8-4
6710 Access Point Horizontal Mount

Vertical Mount

Norand supplies a standard mounting bracket with each access point. The bracket secures the access point to a wall, post, or ceiling. For access points mounted vertically, the type of wall or post determines the hardware needed to mount them. Different surfaces (such as dry-wall, wood, concrete block) require different types of screws and other hardware. For these reasons Norand supplies only a mounting bracket with each access point. The site's personnel must supply the screws and other appropriate hardware.

You must remove the access point's standard mounting plate before you mount the access point on a wall or post. The mounting plate is a template. You can use the template to mark the location of the anchors that secure the mounting plate to the surface. After the mounting plate is securely attached to the surface, the access point is reattached to it.

Figure 8-5 shows an access point mounted vertically with its antenna oriented in an upward position. Norand or certified providers can conduct a formal site survey to determine the proper orientation of antennas for best performance.



1. Mounting bracket
2. 6710 Access Point
3. Mounting bracket (side view)
4. Power cable

Figure 8-5
6710 Access Point Vertical Mount

Power Requirements

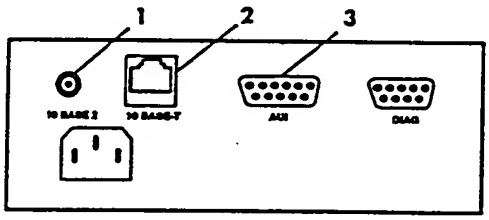
The ac INPUT connector on the bottom panel of the access point is a standard, IEC-type 3-prong connector. The power cord attaches to this connector.

A built-in switching power supply with a source voltage of 85–264 V ac and frequency between 47–63 Hz powers the access point. The power supply supports 110 V ac for operation in domestic markets, and 220 and 240 V ac for international markets. The power supply autosenses the level (110, 220, or 240 V ac) and frequency of the source voltage and operates accordingly.

The dc power cable is 6 feet long. You should locate the access point within 6 feet of the outlet.

Ethernet Connectivity Solutions

The 6710 Access Point connects to the wireless infrastructure through Ethernet and supports 10BASE2, 10BASE5, and 10BASE-T media options. Connections are through the network ports on the access point's bottom panel (Figure 8-6).



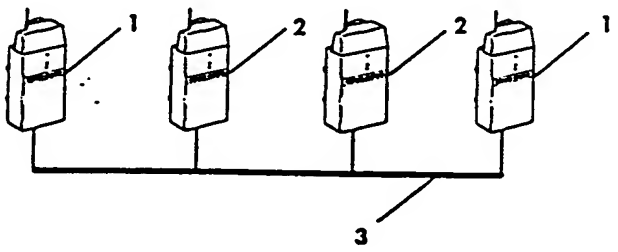
1. BNC port (10BASE2)
2. RJ45 port (10BASE-T)
3. AUI port (10BASE5)

Figure 8-6
6710 Access Point Network Ports

The following pages show how the 6710 Access Point connects to 10BASE2 and 10BASE-T, and how it is installed as a wireless access point.

10BASE2 Connections

The access point can connect to the middle or end of a 10BASE2 segment. Figure 8-7 shows connection options.



1. Access point at end of segment
2. Access point in middle of segment
3. 10BASE2 coax

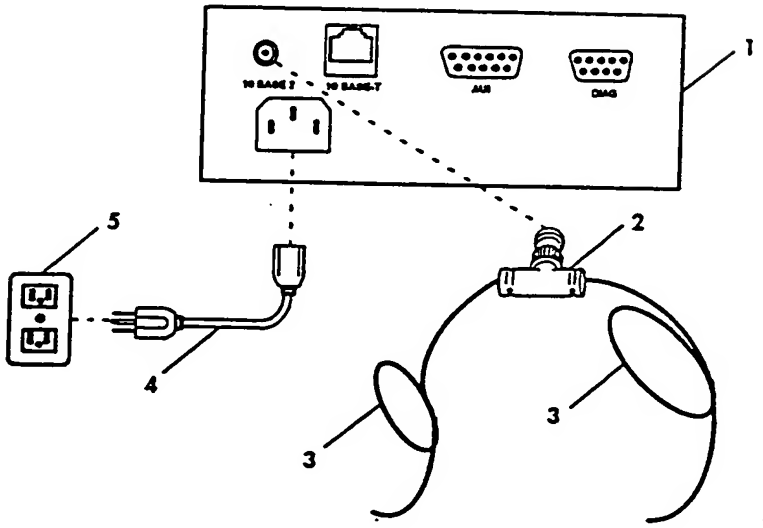
Figure 8-7
6710 Access Point Connection Options

Middle of 10BASE2

An access point that connects to the middle of the 10BASE2 segment requires the following parts:

- ► T-connector
- ► 10BASE2 coax
- ► Power cord
- ► 110, 220, or 240 V ac outlet

Figure 8-8 shows how the parts connect.



1. 6710 Access Point, bottom panel
2. T-connector
3. 10BASE2 coax
4. Power cord (6 feet long)
5. 110, 220, or 240 V ac

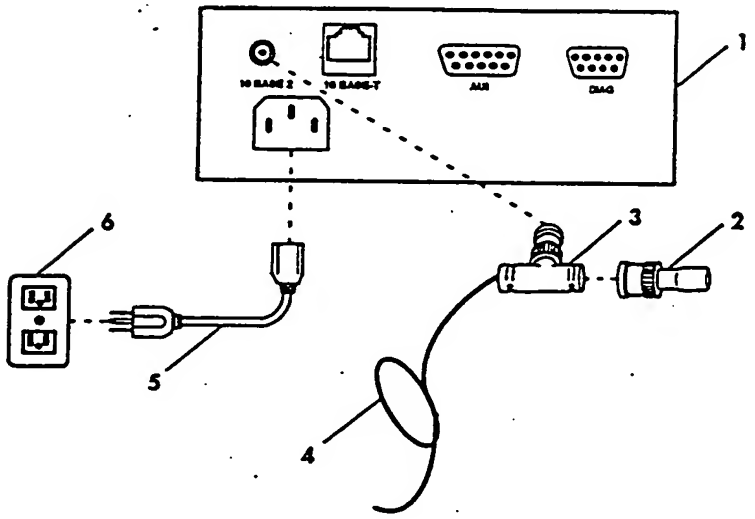
Figure 8-8
6710 Access Point in Middle of 10BASE2

End of 10BASE2

An access point that connects to the end of the 10BASE2 segment requires the following parts:

- T-connector and cable terminator
- 10BASE2 coax
- Power cable
- 110, 220, or 240 V ac outlet

Figure 8-9 shows how the parts connect.



1. 6710 Access Point, bottom panel
2. Cable terminator
3. T-connector
4. 10BASE2 coax
5. Power cord (6 feet long)
6. 110, 220, or 240 V ac

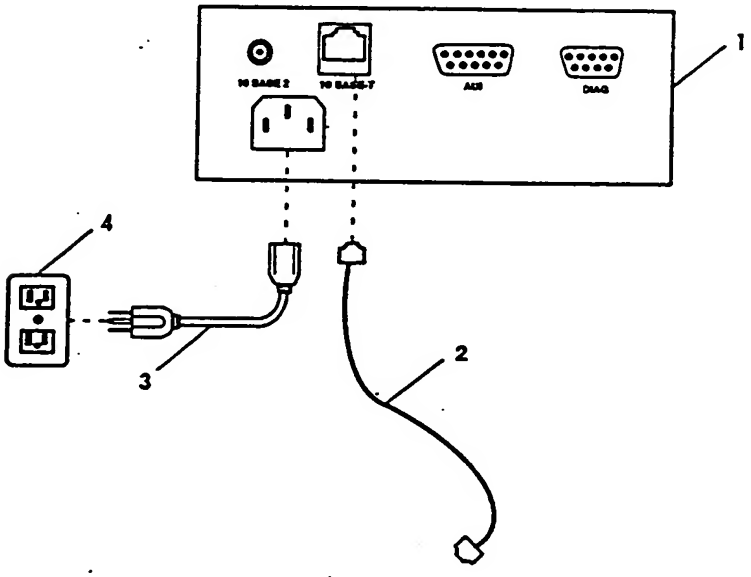
Figure 8-9
6710 Access Point at End of 10BASE2

10BASE-T Connection

An access point that connects to 10BASE-T requires the following parts:

- Cable with RJ45 plugs
- RJ45 jack
- Power cord
- 110, 220, or 240 V ac outlet

Figure 8-10 shows how the parts connect.



1. 6710 Access Point, bottom panel
2. Cable with RJ45 plugs
3. Power cord (6 feet long)
4. 110, 220, or 240 V ac

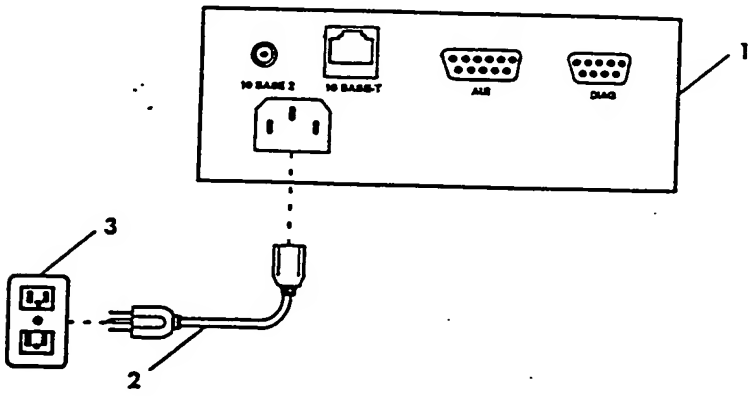
Figure 8-10
6710 Access Point Connected To 10BASE-T

Wireless Access Point Installation

You would typically mount a wireless access point on a ceiling, or high on a wall or post. A wireless access point requires only the following parts:

- Power cord
- 110, 220, or 240 V ac outlet

Figure 8-11 shows how the parts connect.



1. 6710 Access Point, bottom panel
2. Power cord (6 feet long)
3. 110, 220, or 240 V ac

Figure 8-11
6710 Access Point as Wireless Bridge

Installing Host Connectivity Devices

The following pages describe these installation strategies for NORAND gateway products:

- Location
- Mounting options
- Power requirements
- Ethernet connectivity solutions
- Host connectivity solutions

RC4030E Gateway

The following pages describe installation strategies for the RC4030E Gateway.

Location

You would typically locate the RC4030E Gateway next to the host computer in a computer room. The location must meet the requirements in Appendix E, "Host Connectivity Device Specifications."

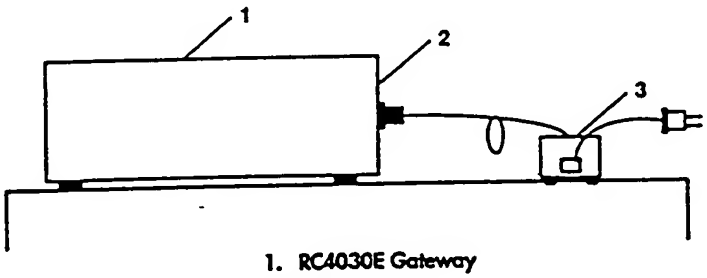
Norand designed the gateway for operation in an enclosed (weatherproof) environment. Norand does not recommend that you locate the gateway in an area that may expose it to harsh operating conditions such as rain, snow, and excessive heat or humidity.

Mounting Options

You can mount the gateway horizontally on a tabletop or vertically on a wall or post. Norand recommends that you mount the gateway vertically so that it will be drip-resistant. A gateway in any other position must be protected from dripping fluids.

Horizontal Mount

The mounting bracket provided with the gateway is not needed for a tabletop installation. When the gateway is on the tabletop, four self-adhesive rubber feet on the gateway's back panel keep it from slipping out of place (Figure 8-12).



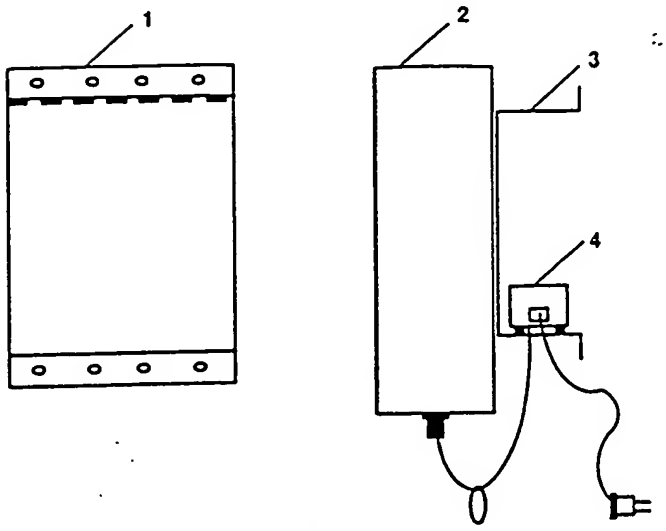
1. RC4030E Gateway
2. Bottom panel
3. NC3100 Power Supply

Figure 8-12
RC4030E Gateway Horizontal Mount

Vertical Mount

Norand provides a mounting bracket with the gateway so that it can mount onto a wall or post. Because the gateway does not require a line of site to the terminal emulation stations, you can mount it at any height. The power supply is usually placed behind the gateway on the mounting bracket.

Figure 8-13 shows a gateway mounted vertically, with the power supply on the bracket.



1. Mounting bracket (front)
2. RC4030E Gateway
3. Mounting bracket (side view)
4. NC3100 Power Supply

Figure 8-13
RC4030E Gateway Vertical Mount

The LEDs on the bottom panel of the gateway are helpful troubleshooting aids. They should be easily visible.

Power Requirements

The RC4030E Gateway requires an NC3100 Power Supply. The power supply has the following characteristics for the United States market:

- Domestic 120 V ac
- 60 Hz power, UL and CSA approval
- Required filtration to meet FCC emissions requirements

The power supply must be located within 6 feet of the gateway and 6 1/2 feet of the power outlet. These distances ensure that the power supply's cables will reach the gateway and outlet. Typically, you would put the power supply on the gateway's wall mounting bracket. If this is infeasible, you can install an extra mounting bracket for the power supply. Norand provides extra mounting brackets.

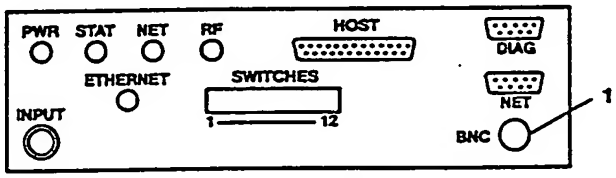
If an outlet cannot be located within 6 feet of the gateway, the dc power cable can be extended. Because of the voltage drop in these cables the extension should not exceed 25 feet. Norand provides assembled dc power extension cables in lengths of 6, 12, and 25 feet.

A different NC3100 Power Supply is used in Europe and other areas having 230 V ac, 50 Hz power with TUV approval. Another type of NC3100 Power Supply is used in Japan and other areas having 100 V ac, 50 or 60 Hz power with MITI approval.

Ethernet Connectivity Solutions

The RC4030E Gateway connects to the wireless infrastructure through Ethernet, and supports 10BASE2 and 10BASE-T media options.

The gateway connects to 10BASE2 through the BNC port on its bottom panel. It connects to 10BASE-T through a media converter. Figure 8-14 shows where the BNC port is located.



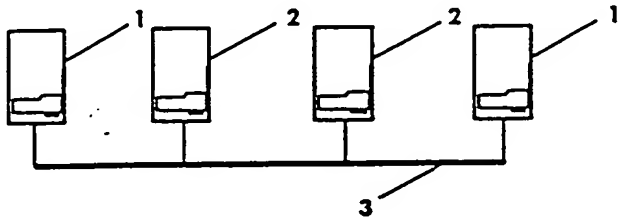
1. BNC port

Figure 8-14
RC4030E Gateway Network Port

The following pages show how the gateway connects to 10BASE2 and 10BASE-T. In some figures the power supply is shown beside the gateway.

10BASE2 Connections

The gateway can connect to the middle or end of a 10BASE2 segment. Figure 8-15 shows connection options.



1. Gateway at end of segment
2. Gateway in middle of segment
3. 10BASE2 coax

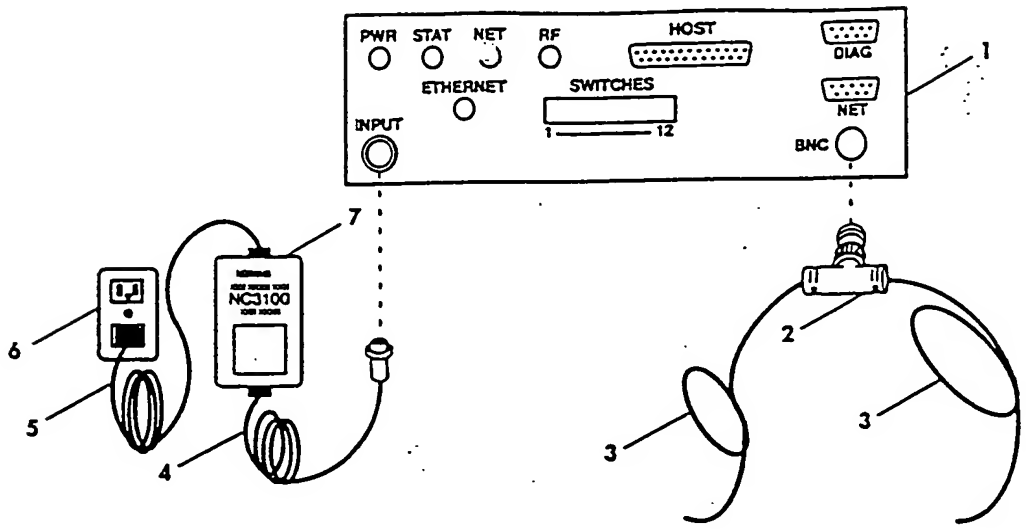
Figure 8-15
RC4030E Gateway Connection Options

Middle of 10BASE2

A gateway that connects to the middle of the 10BASE2 segment requires the following parts:

- T-connector
- 10BASE2 coax
- NC3100 Power Supply and outlet

Figure 8-16 shows how the parts connect.



1. RC4030E Gateway, bottom panel
2. T-connector
3. 10BASE2 coax
4. Power cable, dc (6 feet)
5. Power cable (6 1/2 feet)
6. Outlet
7. NC3100 Power Supply

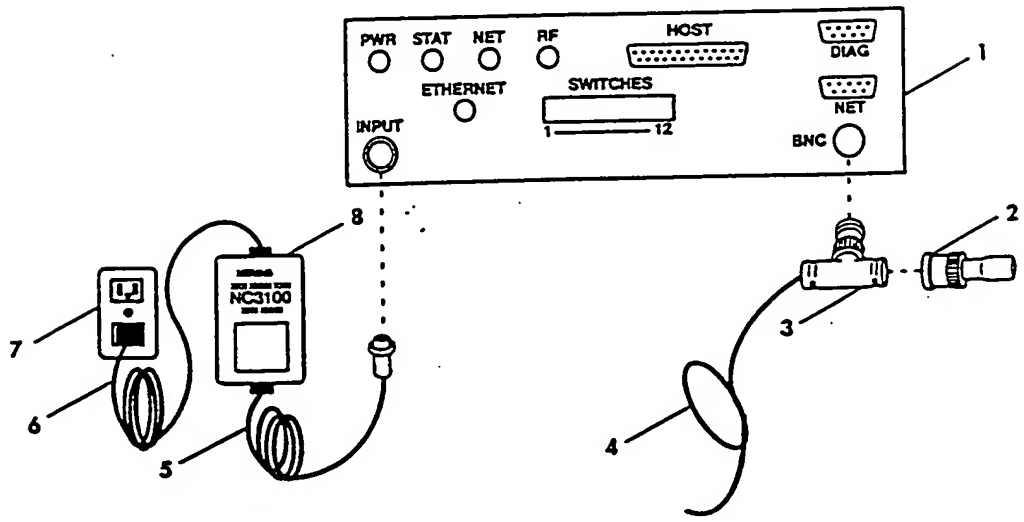
Figure 8-16
RC4030E Gateway in Middle of 10BASE2

End of 10BASE2

A gateway that connects to the end of the 10BASE2 segment requires the following parts:

- T-connector and cable terminator
- 10BASE2 coax
- NC3100 Power Supply and outlet

Figure 8-17 shows how the parts connect.



1. RC4030E Gateway, bottom panel
2. Cable terminator
3. T-connector
4. 10BASE2 coax
5. Power cable, dc (6 feet)
6. Power cable (6 1/2 feet)
7. Outlet
8. NC3100 Power Supply

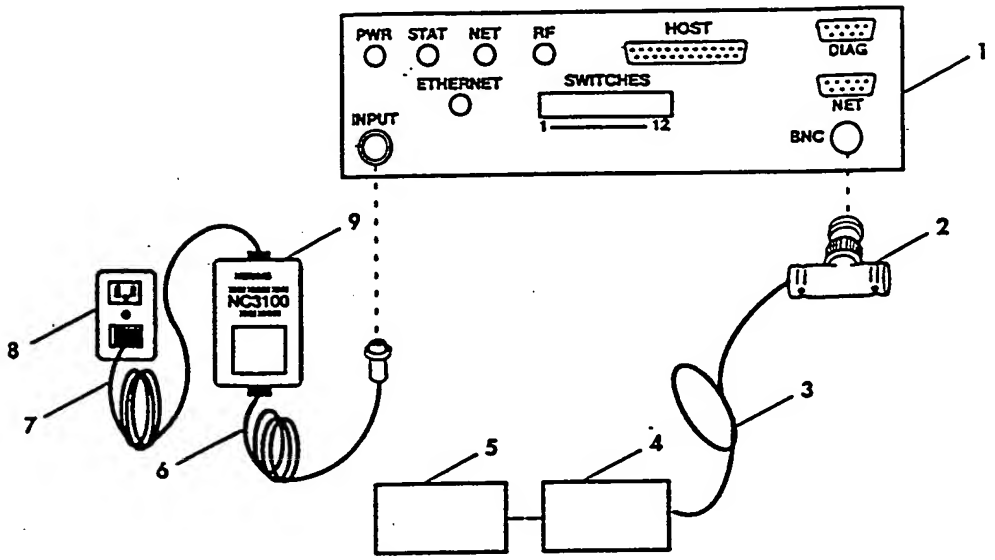
Figure 8-17
RC4030E Gateway at End of 10BASE2

10BASE-T Connection

A gateway that connects to 10BASE-T requires the following parts:

- Media converter
- 10BASE2 coax
- NC3100 Power Supply and outlet

Figure 8-18 shows how the parts connect.

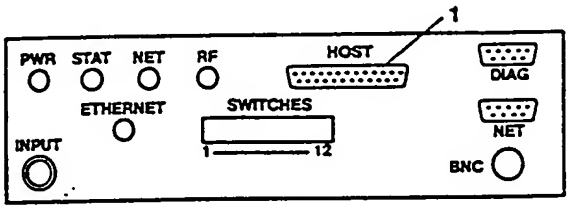


1. RC4030E Gateway, bottom panel
2. T-connector
3. 10BASE2 coax
4. Media converter
5. 10BASE-T hub
6. Power cable, dc (6 feet)
7. Power cable (6 feet)
8. NC3100 Power Supply
9. Outlet

Figure 8-18
RC4030E Gateway Connected to 10BASE-T

Host Connectivity Solutions

Host connection options are V.35 direct and RS-232 direct. The RC4030E Gateway connects, through its 25-pin HOST port, to the 9-pin or 25-pin RS-232 or V.35 port on the host. Figure 8-19 shows where the HOST port is located on the gateway.



1. HOST port

Figure 8-19
RC4030E Gateway HOST Port

The gateway can also connect to the host through modems. Norand provides host and modem cables.

Wireless Network Access Server

Because you would install the Wireless Network Access Server (WNAS) software onto the host, no hardware is needed.

6950 Enterprise Gateway Server

The following pages describe installation strategies for the 6950 Enterprise Gateway Server.

Location

You would typically locate the gateway server next to the host computer in a computer room. The location must meet the requirements in Appendix E.

Norand designed the gateway server for operation in an enclosed (weather-proof) environment. Norand does not recommend that the gateway server be installed in an area that may expose it to harsh operating conditions such as rain, snow, and excessive heat or humidity.

Mounting Options

You can mount the gateway server horizontally on a tabletop. A mounting bracket is not needed for a tabletop installation. When the gateway server is on the tabletop, four self-adhesive rubber feet on its bottom panel keep it from slipping out of place. An optional wall mounting bracket mounts the gateway server on a wall.

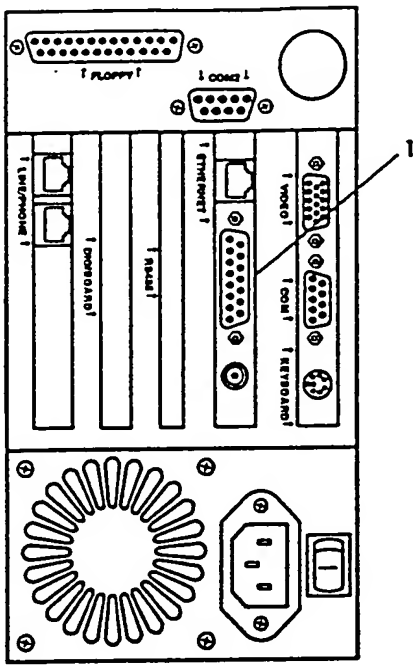
Power Requirements

An internal 65 watt power supply powers the gateway server. The power supply requires an ac power outlet. The power supply autosenses the level (110, 220, or 240 V ac) and frequency of the source voltage and operates accordingly.

You must locate the gateway server within 7 feet of the power outlet. This distance ensures the power cord reaches the gateway server and the outlet.

Ethernet Connectivity Solutions

The gateway server connects to the wireless infrastructure through Ethernet, and supports 10BASE2, 10BASE5, and 10BASE-T media options. Connections are through the network ports on its installed Ethernet adapter card (Figure 8-20).



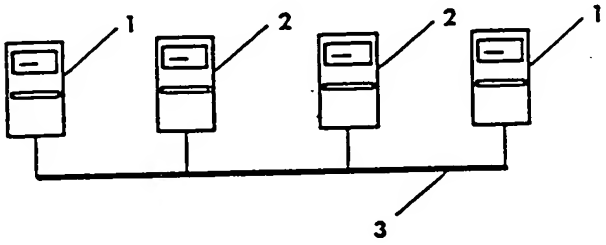
1. Network ports on Ethernet adapter card

Figure 8-20
6950 Enterprise Gateway Server Network Ports

The following pages show how the gateway server connects to 10BASE2 and 10BASE-T.

10BASE2 Connections

The gateway server can connect to the end or middle of a 10BASE2 segment. Figure 8-21 shows connection options.



1. Gateway server at end of segment
2. Gateway server in middle of segment
3. 10BASE2 coax

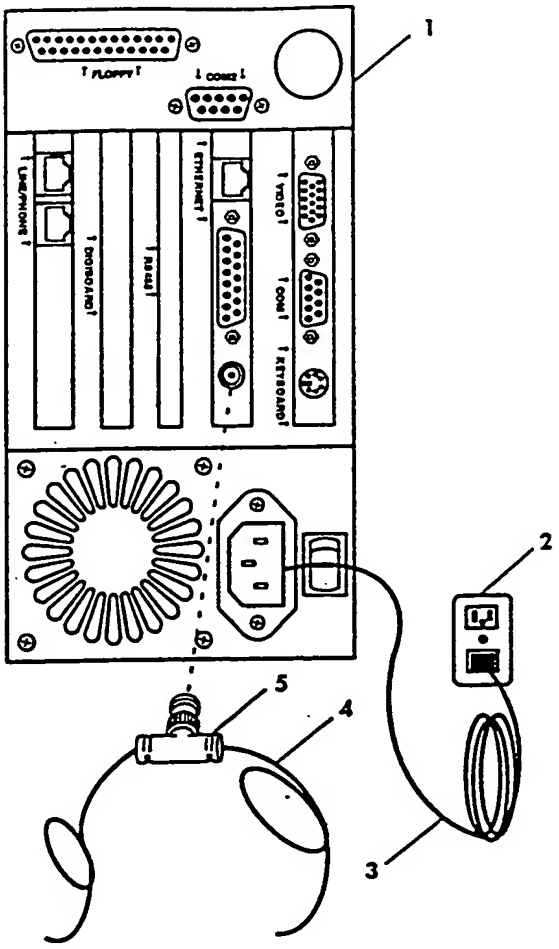
Figure 8-21
6950 Enterprise Gateway Server Connection Options

Middle of 10BASE2

A gateway server that connects to the middle of the 10BASE2 segment requires the following parts:

- T-connector
- 10BASE2 coax
- Power cord and outlet

Figure 8-22 shows how the parts connect.



1. Gateway server, rear panel
2. Outlet
3. Power cord (7 feet)
4. 10BASE2 coax
5. T-connector

Figure 8-22
6950 Enterprise Gateway Server in Middle of 10BASE2

End of 10BASE2

A gateway server that connects to the end of the 10BASE2 segment requires the following parts:

- T-connector and cable terminator
- 10BASE2 coax
- Power cord and outlet

Figure 8-23 shows how the parts connect.

10BASE-T Connection

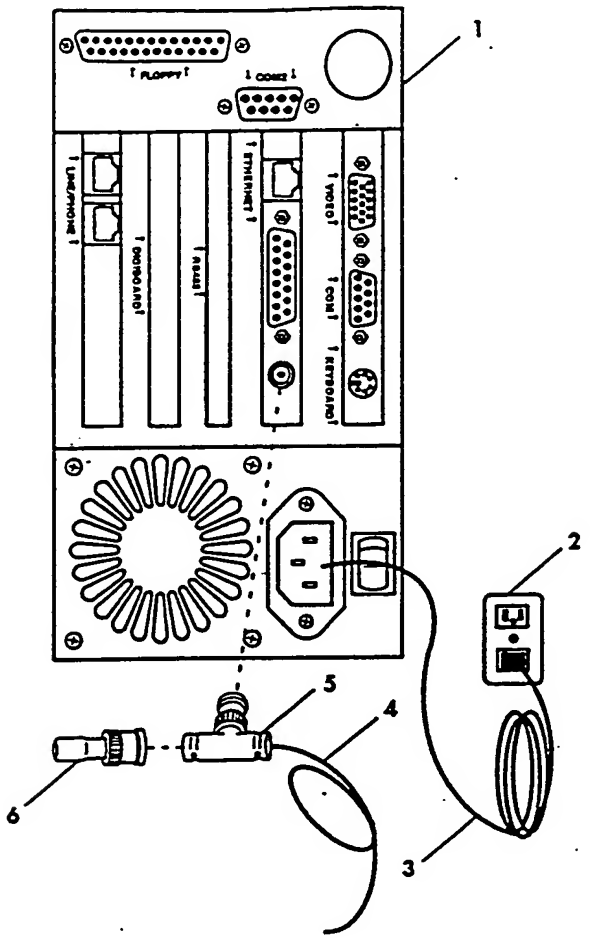
A 6950 Enterprise Gateway Server that connects to 10BASE-T requires the following parts:

- Cable with RJ45 plugs
- RJ45 jack
- Power cord and outlet

Figure 8-24 shows how the parts connect.

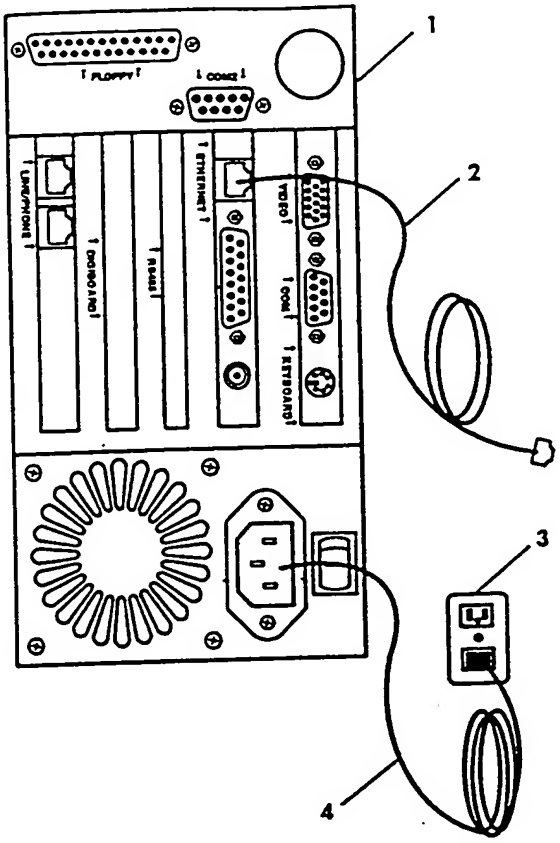
Host Connectivity Solution

Because the gateway server connects to the host through the Ethernet medium, no host cables are needed.



1. Gateway server, rear panel
2. Outlet
3. Power cord (7 feet)
4. 10BASE2 coax
5. T-connector
6. Cable terminator

Figure 8-23
6950 Enterprise Gateway Server at End of 10BASE2



1. Gateway Server, rear panel
2. Cable with RJ45 plugs
3. Outlet
4. Power cord (7 feet)

Figure 8-24
6950 Enterprise Gateway Server Connected to 10BASE-T

Disconnecting Fixed-end Devices

You can disconnect the 6710 Access Point, RC4030E Gateway, and 6950 Enterprise Gateway Server from a network segment without disrupting service. Disconnecting the fixed-end device from 10BASE2 involves disconnecting the T-connector from the device but leaving the 10BASE2 cables connected to the T-connector. You must attach a cable terminator to a T-connector at the end of a cable.

Disconnecting a fixed-end device from 10BASE-T involves pulling the cable with the RJ45 plugs from the fixed-end device and RJ45 jack. Pulling this cable disables only the fixed-end device at the end of the cable.

Installation Examples

The rest of this section contains examples of three different types of installations:

- Warehouse site installation with 10BASE2 coax
- Retail site installation with 10BASE2 coax

The examples include a diagram of the installation and a breakdown of the parts and cabling that would be required.

Warehouse Site

Figure 8-25 shows an example of an installation for a warehouse site. In the figure "AP" is a 6710 Access Point with a 900 MHz or UHF NIC, "GW" is an RC4030E Gateway, and "R" is a repeater. The Ethernet medium is 10BASE2 coax.

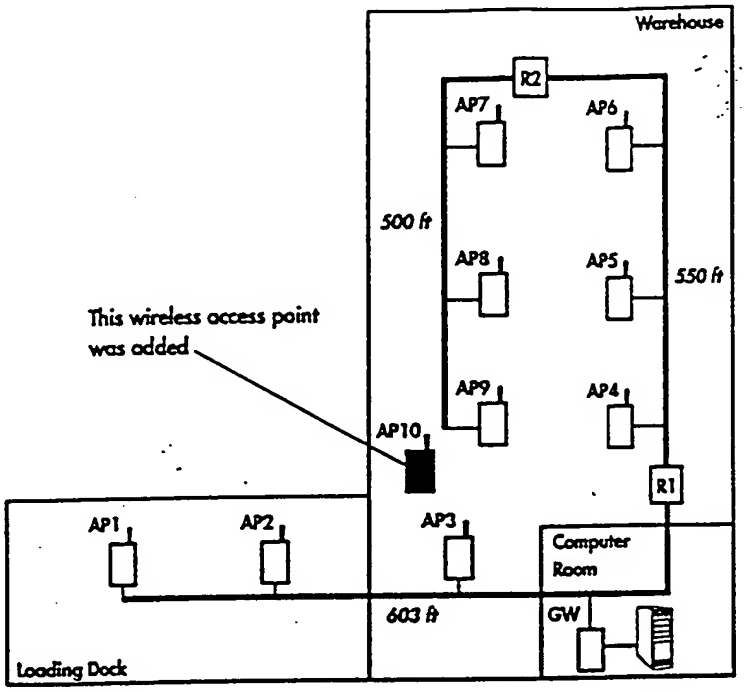


Figure 8-25
Warehouse Site Installation With 10BASE2

A survey for this site revealed two issues. One was the marginal coverage between AP2 and AP3. The other was the possibility of a broken cable disrupting service. The cost of a fully redundant system at this site was not feasible. (Redundancy is providing duplicate devices to immediately take over the function of equipment that fails.)

To resolve the marginal coverage issue, a wireless access point (AP10) was added. The wireless access point covers the area between AP2 and AP3. It also resolves the broken cable issue for the following reasons:

- It provides alternate, wireless routes between AP3 and AP2, between AP9 and AP2, and between AP3 and AP9.
- It covers a cable break between GW and AP3, or between AP3 and AP2.
- It provides communication to GW if a break occurs between GW and R1, or between R1 and AP4.

The wireless access point covers any cable break. For example:

- If the cable from AP6 to AP7 broke, AP6, AP5, and AP4 would communicate with GW through R1.
- AP7, AP8, and AP9 would take the wireless route (AP10 to AP3 and then to GW).

Determining the Parts Required

The following chart lists the parts needed to connect each NORAND fixed-end device to the 10BASE2 cable.

Code	Description	Segment Location	Parts Required
AP1	Access point	End	T-connector, cable terminator
AP2	Access point	Middle	T-connector
AP3	Access point	Middle	T-connector
AP4	Access point	Middle	T-connector
AP5	Access point	Middle	T-connector
AP6	Access point	Middle	T-connector
AP7	Access point	Middle	T-connector
AP8	Access point	Middle	T-connector
AP9	Access point	End	T-connector, cable terminator
AP10	Access point	(Wireless)	(None)
GW	Gateway	Middle	T-connector

Determining Cable Amounts

The warehouse site installation needs about 1,653 feet of coaxial cable to join all network devices. However, segment lengths for 10BASE2 can be no longer than 607 feet. The length was divided as follows:

- 603 feet between AP1 and R1
- 550 feet between R1 and R2
- 500 feet between R2 and AP9

These three segments are joined by two repeaters.

Bill of Materials

A bill of materials (BOM) for the cable and NORAND fixed-end devices in this installation would resemble the following chart.

BOM Item #	Description	Quantity
1	RG58 A/U 10BASE2 coaxial cable	1,653 ft
2	6710 Access Point	10
3	RC4030E Gateway	1
4	Extra mounting bracket (if needed for RC4030E Gateway's power supply)	1
5	Remote antenna for AP10	1
6	NEMA enclosures for AP1 and AP2	2

Retail Site

Figure 8-26 shows an example of an installation for a small retail store. In the figure "AP" is a 6710 Access Point with a Proxim 2.4 GHz NIC and "GW" is an RC4030E Gateway. The Ethernet medium is 10BASE2 coax.

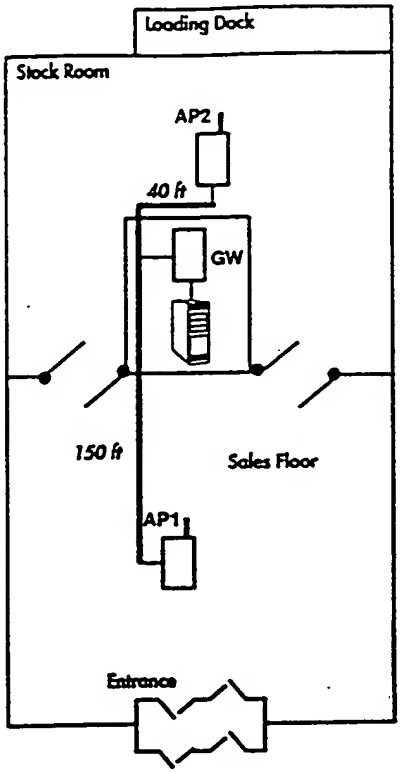


Figure 8-26
Retail Site Installation With 10BASE2

A single 6710 Access Point could cover the sales floor and the stock room. However, the site survey revealed that the concrete wall between the sales floor and stock room prevented effective coverage of both areas from one access point. Because complete coverage is required for the loading dock and front part of the sales floor, access point AP2 was added.

Determining the Parts Required

The following chart lists the parts needed to connect each NORAND fixed-end device to the 10BASE2 cable.

Code	Description	Segment Location	Parts Required
AP1	Access point	End	T-connector, cable terminator
AP2	Access point	End	T-connector, cable terminator
GW	Gateway	Middle	T-connector

Determining Cable Amounts

The retail installation needs about 190 feet of coaxial cable to join all network devices. This is under the maximum segment length for 10BASE2 (607 feet), so no repeater is needed.

Bill of Materials

A BOM for the cable and NORAND fixed-end devices in this installation would resemble the following chart.

BOM Item #	Description	Quantity
1	RG58 10BASE2 A/U coaxial cable	190 ft
2	6710 Access Point	2
3	RC4030E Gateway	1
4	Extra mounting bracket (if needed for RC4030E Gateway's power supply)	1

Section 9

System Management

About This Section

This section describes configuration and management for NORAND® wireless infrastructure components.

Access Point Setup and Configuration

System software parameters for the 6710 Access Point reside in the access point's FLASH ROM. You would use the parameters to set IP addresses, network spanning tree options (such as LAN ID, netname or security ID, and root priority), and other operational features.

You initially configure the 6710 Access Point locally through the access point's DIAG port. After you configure the access point locally, you can access its configuration menus locally or through a remote TELNET session over the network backbone. Complete information about establishing a TELNET session is in the *6710 Access Point User's Guide (NPN: 961-047-081)*.

You do not need special equipment to configure the 6710 Access Point through a TELNET session. However, the access point must be connected to the Ethernet medium (or attached through a wireless link) and have its IP address set as a minimum. (This address must be set locally through the DIAG port.) To manage the access point from a remote location, you would establish a TELNET session with the access point's IP address.

Software Download

Software can be downloaded to an access point through its configuration menus or through SNMP.

Configuration Menus

You can download a new version of system software to a 6710 Access Point through its configuration menus. You can access the menus locally through the access point's DIAG port, or remotely over the network through a PC running server software and TELNET. You can then transfer files from the PC server to the access point (the client device). This feature enables you to download, from a central location, a new version of system software to each access point on a network.

The PC server physically connects to the LAN or to an Ethernet modem, which provides connection to the LAN. The server software Norand recommends for DOS and Windows is TFTP by FTP Software, Inc. All file transfers between the PC TFTP server and the TFTP client (the access point) are through User Datagram Protocol (UDP) packets and TFTP's binary transfer mode.

You establish a TELNET session with the access point's IP address while the TFTP server software is running on the PC. This connection lets you access the TFTP server (through the GET command) and the access point's command line interface for the configuration menus. The series of steps required to download the software to the access point repeats for each access point.

For diagnostic purposes, the access point's command line interface supports commands that show the current status of the file system and allow the file system to be reset if necessary.

The access point operates normally throughout the software download process. While you are downloading a new version of software to the access point, it continues to use the previous version of software until you reboot it through the *reboot* command. After the access point reboots, it uses the new version of software.

SNMP

Software download can also be done through SNMP. This allows a set of access points to automatically perform a set of commands. It also allows the software to be downloaded by multiple access points at a particular time. This method requires a "download script file," which each access point uses as a source of the commands to execute. The "download script file and the software must be on the TFTP server, which could be a PC or an access point.

Setup and Configuration of Host Connectivity Devices

The following pages describe system management for the RC4030E Gateway, 6910 Integrated Gateway/Access Point, WNAS, and 6950 Enterprise Gateway Server.

RC4030E Gateway

System software parameters for the RC4030E Gateway reside in the gateway's FLASH ROM. The parameters set IP addresses, the host type (such as 3270), and communication options (such as group chaining and compression).

You initially configure the RC4030E Gateway locally through its DIAG port. You can then access its configuration options locally or through a remote TELNET session. You do not need special equipment to configure the gateway through a TELNET session. However, the gateway must be connected to the Ethernet medium and have its IP address set as a minimum. To manage the gateway from a remote location, you would establish a TELNET session with the gateway's IP address. Complete information about establishing a TELNET session is in the *RC4030E Gateway User's Guide (NPN: 961-047-087)*.

6910 Integrated Gateway/Access Point

System software parameters for the 6910 Integrated Gateway/Access Point reside in the gateway/access point's FLASH ROM. The parameters set IP addresses, the NORAND Native host type, and communication options (such as group chaining and compression). The parameters also set access point bridging and radio options.

System management for the gateway/access point is the same as for the RC4030E Gateway and 6710 Access Point. Complete information about the gateway/access point is in the *6910 Integrated Gateway/Access Point User's Guide (NPN: 961-047-095)*.

WNAS

After you install WNAS onto the host, you can configure it to meet your site's requirements. Use WNAS configuration parameters to do the following:

- Configure runtime options (such as RS-232 parameters)
- Define the applications to be run from the terminal emulation station
- Determine the menu that each terminal emulation station should display when it powers up
- Set wireless station-specific configurations (such as which menu to use for a specific wireless station number)

You initially configure WNAS locally on the host. You can then access its configuration menus locally or through a remote TELNET session. You do not need special equipment to configure WNAS through a TELNET session. However, WNAS must have an IP address set as a minimum. To manage WNAS from a remote location, you would establish a TELNET session with the IP address. Complete information about establishing a TELNET session is in the *Wireless Network Access Server User's Guide (NPN: 961-051-006)*.

6950 Enterprise Gateway Server

You can configure network options for the 6950 Enterprise Gateway Server through one of the following methods:

- Terminal emulation station within range of the 6710 Access Point
- TELNET session
- Keyboard and monitor attached to the gateway server
- Dumb terminal plugged into the COM2 port

You initially configure the gateway server locally. You can then access its configuration menus locally or through a remote TELNET session. You do not need special equipment to configure the gateway server through a TELNET session. However, the gateway server must be connected to the Ethernet medium and have its IP address set as a minimum.

To manage the gateway server from a remote location, you would establish a TELNET session with the gateway server's IP address. Complete information about establishing a TELNET session is in the *6950 Enterprise Gateway Server User's Guide (NPN: 961-047-091)*.

SNMP

6710 Access Points and RC4030E Gateways are manageable through SNMP. SNMP is an industry-standard protocol that provides a way for network management platforms to query other network devices for status and other device information. The information is typically system identification data, or counters indicating error rates or performance measures in the network device being queried.

SNMP uses the UDP transport-level protocol to provide communications between a network management station and the agent that resides in the managed object. RFC1157 defines the SNMP.

Elements of the SNMP network management system are:

- Network management platform
- SNMP agent
- MIB
- Private NORAND MIBs
- TCP/IP stack

Network Management Platform

A network management platform is a collection of software modules that use SNMP (and the list of objects which can be obtained) to automatically retrieve, display, save, or analyze data. The platform is installed on a network management station, which must meet the requirements outlined in the management platform's user manual.

Norand recommends the OpenView for Windows by Hewlett-Packard (HP) platform to provide network management capability for the open wireless LAN. HP OpenView is a standards-based network management platform. Complete information about HP OpenView for Windows is in the *NORAND Open Wireless LAN with HP OpenView for Windows User's Guide (NPN: 961-051-009)*.

NORAND OWLView for Windows is a separate management application for HP OpenView. OWLView helps manage the open wireless LAN by showing wired and wireless components and connections of NORAND LAN devices. OWLView also shows wireless stations communicating through the open wireless LAN, and periodically updates maps with the status of NORAND devices and connections. Complete information is in the *OWLView for HP OpenView for Windows User's Guide (NPN: 961-051-010)*.

SNMP Agent

An SNMP agent resides at the managed device (such as the 6710 Access Point). The agent accepts SNMP requests from an SNMP network management platform and responds with the requested data. The SNMP agent also services SNMP SET requests and sends unsolicited messages (called traps) when a predefined event occurs.

MIB

A MIB defines the management information that the device supports. MIB-II is the standard MIB defined for SNMP over TCP/IP.

Resident agents for 6710 Access Points and RC4030E Gateways support MIB-II for TCP/IP–based internets. MIB-II is a set of objects an SNMP network management platform can query or set in the SNMP agent of a network device, such as a router or 6710 Access Point. MIB-II provides information about the device, and TCP/IP and SNMP activity for the device.

MIBs are written in Abstract Syntax Notation.1 (ASN.1). ASN.1 is defined in ISO documents 8824.2 and 8825.2. ASN.1 is a machine-independent data definition language that provides an interface to the underlying management information in a system. RFC1155 defines ASN.1 formats, and RFC1213 defines MIB formats.

Because a MIB is written in ASN.1, it can be directly imported into any SNMP network management platform. The MIB defines and describes the management data the fixed-end devices support.

Complete information about MIBs for the 6710 Access Point and RC4030E Gateway is in the *NORAND Management Information Base Reference Manual (NPN: 977-051-002)*.

Private NORAND MIBs

Each 6710 Access Point and RC4030E Gateway maintains a set of private NORAND MIBs. These MIBs apply to both of these devices, or only to a specific device. The MIBs are installed with the network management platform.

A tree structure stores management data (objects). Object identifiers (OIDs) are assigned based on the position of the object in the tree. Standard objects (such as MIB-II) register with the Internet Assigned Numbers Authority (IANA). The IANA is the central registry for various internet protocol parameters such as port, protocol, and enterprise numbers, and options, codes, and types.

Enterprises can register with the IANA for an Enterprise ID, which gives the enterprise its own subtree in the the standard object tree. The Enterprise ID for Norand is 469.

TCP/IP Stack

A TCP/IP stack must be installed on the network management station if it does not already have one. Norand recommends the PC/TCP TCP/IP stack by FTP Software. The stack is available through Norand.

Appendix A

Radio Options

About This Appendix

This appendix describes wireless technology options for the wireless infrastructure. NIC specifications, international frequencies, and data rates are also in this appendix.

Wireless Technology Options

Wireless technology options for the wireless infrastructure are 900 MHz multimode RF, synthesized UHF, and 2.4 GHz frequency hopping (Proxim RangeLAN2). Norand is also developing product capabilities compatible with the emerging IEEE 802.11 standard for wireless LANs, which is currently slated for approval by late 1996. Contact a Norand representative for the current status.

900 MHz Radio Option

The following chart lists NICs and their NORAND® model names for the 900 MHz radio option.

NIC*	Device	Model Name
Type III	6710 Access Point	RM160
	PEN*KEY® 6400	RM160
	PEN*KEY 6600	RM160
	PEN*KEY 6100	RM160
Radio modules	RT1100	RM60, RM70, RM70LR (radio modules)
	RT1700	RM60, RM70, RM70LR (radio modules)

**Consult a Norand representative for availability.*

NIC Specifications

Following are networking specifications for the 900 MHz NIC.

Frequency band:	902–928 MHz spread spectrum direct sequence
Range:	Up to 1300 feet line of sight
Coverage:	100,000–350,000 square feet in typical indoor installations
Data rate:	90, 225, or 450 Kbps (depends on installation)
Channelization:	7 @ 90 Kbps, 1 @ 225, 450 Kbps
Client driver:	ODI
Software compatibility	Requires NORAND communications software resident in the access point
Output power:	250 mW
MAC protocol:	NORAND open wireless LAN MAC radio protocol
Regulatory compliance:	FCC 15.247; Industry Canada RSS 210 (Consult a Norand representative for availability.)

Frequencies and Data Rates

NORAND wireless devices with the 900 MHz option can operate in Australia and in most countries in North and South America. Table A-1 lists various countries and their 900 MHz frequencies. Contact a Norand representative for current information about countries in which the product is approved for use and countries in which submission for type approval is planned.

Table A-1
900 MHz Frequencies – International

Country	Frequencies (MHz)
Australia	919.5, 921.5, 923.5
Canada	907.5, 910.0, 912.5, 915.0, 917.5, 920.0, 922.5

Table A-1 (Continued)
900 MHz Frequencies – International

Country	Frequencies (MHz)
Mexico	907.5, 910.0, 912.5, 915.0, 917.5, 920.0, 922.5
United States	907.5, 910.0, 912.5, 915.0, 917.5, 920.0, 922.5

Table A-2 lists corresponding data rates for Canada, Mexico, and the United States.

Table A-2
Corresponding Data Rates – Canada, Mexico, and United States

Frequency (MHz)	Data Rate (Kbps)
907.5	90
910.0	90
912.5	90
915.0	90
917.5	90
920.0	90
922.5	90
902–928	225
902–928	450

Table A-3 lists corresponding data rates for Australia.

Table A-3
Corresponding Data Rates – Australia

Frequency (MHz)	Data Rate (Kbps)	Channel
919.5	90	34
921.5	90	38
923.5	90	42

Synthesized UHF Radio Option

The following chart lists NICs and their NORAND model names for the synthesized UHF radio option.

NIC*	Device	Model Name
Type II (tethered)	6710 Access Point	RM111
	PEN*KEY 6400	RM111
	PEN*KEY 6600	RM111
Mini-ISA	PEN*KEY 6100	RM211
	RT1100	RM11, RM31 (radio modules)
	RT1700	RM11, RM31 (radio modules)

**Consult a Norand representative for availability.*

NIC Specifications

Following are networking specifications for the synthesized UHF NIC.

Frequency band:	450–470 MHz, four-level FSK (frequency shift keying)
Range:	Up to 3500 feet line of sight
Coverage:	800,000 square feet in typical indoor installations
Data rate:	19.2 Kbps (14.4 Kbps with forward error correction)
Channelization:	20 KHz or 25 KHz
Client driver:	ODI
Software compatibility	Requires NORAND communications software resident in the access point
Output power:	500 mW
MAC protocol:	NORAND open wireless LAN MAC radio protocol
Regulatory compliance:	FCC Parts 15, 90; Industry Canada RSS 119; ETS 300-220; FTZ 2014 (Germany); CE Mark (Europe) (Consult a Norand representative for availability)

Frequencies

NORAND wireless devices with the synthesized UHF option can operate in Europe, the Pacific Rim (except Japan), Australia, and most countries in North and South America. Contact a Norand representative for current information about countries in which the product is approved for use and countries in which submission for type approval is planned.

Proxim 2.4 GHz Radio Option

The following charts list NICs and their NORAND model names for the Proxim 2.4 GHz radio option.

Access Point NIC*	Device	Model Name
Type III	6710 Access Point	RM180

**Requires NORAND communications software resident in the access point.*

Wireless Station NIC*	Device	Model Name
Type III	PEN*KEY 6400	RM180
	PEN*KEY 6600	RM180
Type II	Laptops and notebooks ..	RM185
Mini-ISA	PEN*KEY 6100	RM280
	RT1100	RM80, RM90, RM90LR (radio modules)
	RT1700	RM80, RM90, RM90LR (radio modules)
ISA	Desktops	RM380

**Consult a Norand representative for availability.*

NIC Specifications

Following are networking specifications for the Proxim 2.4 GHz NIC.

Frequency band:	2.401–2.480 GHz spread spectrum frequency hopping
Range:	Up to 500 feet line of sight
Coverage:	25,000 square feet (2,322 square meters) in typical indoor installations
Data rate:	800 Kbps or 1.6 M bps, manual or autoselecting
Client drivers:	ODI and NDIS (version 2.0.1 for DOS and Windows)
6710 Access Point:	Requires NORAND communications software resident in the access point
Ethernet compatibility:	Ethernet packet types and Ethernet addressing
Output power:	100 mW
MAC protocol:	RangeLAN2
Regulatory compliance:	FCC 15.247; Industry Canada RSS 210; European Union ETS 300-328 (Consult a Norand representative for availability.)

Frequencies and Data Rates

NORAND wireless devices with the 2.4 GHz option can operate in most areas that allow use of spread spectrum wireless communications at 2.4 GHz, including Australia and countries in North and South America, Europe, and Asia. Table A-4 lists various countries and their corresponding 2.4 GHz frequencies and data rates. Contact a Norand representative for current information about countries in which the product is approved for use and countries in which submission for type approval is planned.

Table A-4
Proxim 2.4 GHz Frequencies and Data Rates – International

Country	Frequency Band (GHz)	Data Rate (Kbps)
Australia	2.401–2.443	800 or 1600
Canada	2.402–2.480	800 or 1600
Denmark	2.407–2.449	800 or 1600
France	2.447–2.480	800 or 1600
Germany	2.407–2.449	800 or 1600
Hong Kong	2.402–2.480	800 or 1600
Italy	2.407–2.449	800 or 1600
Japan	2.473–2.495	800 or 1600
Mexico	2.452–2.472	800 or 1600
Spain	2.407–2.449	800 or 1600
United Kingdom	2.407–2.449	800 or 1600
United States	2.402–2.480	800 or 1600

Radio Kits

Standard radio kits are available from Norand as factory-installed options. Different radio kits allow the radio network to be customized to provide various data throughput and performance tradeoffs. Consult a Norand representative for the radio kit options currently available.

In accordance with regulations, radio kits are usually shipped with standard antenna kits that use a unique RF (radio frequency) connector. Replacement antennas are available from Norand.

Remote antenna kits are also available from Norand. In accordance with regulations, remote antenna kits must be installed by Norand or other qualified personnel. Only antennas furnished by Norand can be used with NORAND access points.

Performance Tradeoffs

▶ NOTE: *Norand or certified providers can conduct a site survey to help you choose the best radio option for your site. Section 8, "Installation," discusses site surveys.*

When determining the type of radio or radios to use, you must consider the size and physical layout of the site and the amount of traffic that will flow through the network. Note that radio range decreases as radio frequency and data speed increase.

The 900 MHz option is a good compromise between coverage and data rate. It is a good choice for large populations of stations, or for users who want high performance. For PEN*KEY computers, notebooks, and laptops, it is recommended for light to medium density data applications in factories and other large spaces. The 900 MHz radio does not require a site license.

The UHF option has the best coverage but the lowest data rate. It is a good choice for low to medium populations of terminal emulation stations. The UHF radio requires a site license.

The Proxim 2.4 GHz option has the highest data rate but the lowest coverage. It is a good choice for when file transfers are regular or where users have written their own applications, which puts a significant amount of traffic on the air. For PEN*KEY computers, notebooks, and laptops, it is recommended for information-intensive applications requiring high throughput.

Radio and Scanner Modules

Radio and scanner modules for terminal emulation stations in the RT1100 and RT1700 Series are interchangeable. For example, you can change a 900 MHz radio on an RT1700 to a 2.4 GHz radio by changing radio modules; you do not need to replace the entire terminal emulation station. The following chart describes radio modules and scanning capabilities.

Module	Description
RM11	UHF radio
RM31	UHF radio with integrated, standard-range scanner
RM60	900 MHz radio
RM70	900 MHz radio with integrated, standard-range scanner
RM70LR	900 MHz radio with integrated, standard-range scanner (such as used on a forklift)
RM80	2.4 GHz radio
RM90	2.4 GHz radio with integrated, standard-range scanner
RM90LR	2.4 GHz radio with integrated, long-range scanner (such as used on a forklift)

The type of module attached to the terminal emulation station determines the model. For example, an RT1700 with a 2.4 GHz radio module is a model RT1780.

The user activates the scanner module through one of these methods:

- Scanning buttons integrated into the radio module
- Scan button on the RT1700 and PEN*KEY 6400 Computer
- Optional scanning handle for the RT1100 and RT1700

Scanner modules support these bar code symbologies:

ABC Codabar
Codabar
Code 39
Code 93
Code 128
EAN
EAN with add-ons
Encoded Code 39
Extended Code 39
Interleaved 2 of 5
Plessey
Straight2 of 5
UPC
UPC with add-ons

Appendix B

Recommended Network Products

About This Appendix

If you are purchasing a complete networking solution from Norand, refer to this appendix for the products Norand recommends for use with the open wireless LAN. If you are already using products by other vendors, the open wireless LAN should operate correctly with those products.

Modems, Hubs, Bridges, and Transceivers

Products listed in the following chart are available through Norand. For more information about a product refer to its user guide or contact Norand.

Product (Vendor)	Product Name
Ethernet modem (Shiva)	NetModem/E
Hubs (3COM)	LinkBuilder FMS II 12-port twisted pair LinkBuilder FMS 10-port BNC FMS LinkBuilder II 6-port fiber
Hub options (3COM)	Fiber Optic Interface Module Redundant Power System LinkBuilder FMS II Management Module

(Continued on next page)

Product (Vendor)	Product Name
Bridge (3COM)	LinkBuilder Bridge MicroModule
Interbuilding bridge (Proxim)	RangeLINK 2021 with yagi antenna
Transceivers (Transition Networks)	10BASE-T to 10BASE2 10BASE2 to 10BASEF 10BASEF to 10BASE-T

Other Products and Configurations

Following are products and configurations that require special approval through Norand for use with the open wireless LAN. Contact the Advanced Technology Group at Norand for more information.

FDDI
100VGAnyLAN
Fiber Optic Inter Repeater Link (FOIRL)
Routers
Asynchronous Transfer Mode (ATM)
10BASE-T switch
10BASE-F switch

Appendix C

ODI and NDIS Driver Configurations

About This Appendix

This appendix contains examples of ODI and NDIS driver configurations for a PEN*KEY® 6100 Computer with the Proxim 2.4 GHz radio option. The configurations shown are for a Novell NetWare 4.x client and a TCP/IP host using PC/TCP networking software by FTP Software, Inc. NetWare uses only the ODI driver. PC/TCP can use the ODI driver or the NDIS driver.

ODI Driver for NetWare and TCP/IP

The ODI driver for the PEN*KEY 6100 Computer is RL2OEM.COM. The driver uses the network parameters in the NET.CFG file. To load the driver you would load — into AUTOEXEC.BAT — LSL.COM (the link support layer), RL2OEM.COM, and then the protocol stack or driver (IPXODI.EXE for NetWare, and ETHDRV.EXE or VXDINIT.EXE for TCP/IP).

NET.CFG

Following is an example of a NET.CFG file.

```
LINK DRIVER RL2OEM
        INT                     15
# This is the IRQ and I/O base address used by the 2.4 GHz radio.
        PORT                    3F0
        BUS_MODE                1
# STATION_TYPE 0 means station only, 1 is alternate master, 2 is master
# always.
        STATION_TYPE            0
        DOMAIN                  3
        SUBCHANNEL              1
        CHANNEL                 1
# INACTIVITY_MIN/SEC set to 0 will keep the station awake always.
# INACTIVITY_MIN/SEC set to anything > 0 the radio will snooze and will not
# reliably respond to broadcasts.
        INACTIVITY_MIN          0
        INACTIVITY_SEC          0
#       INACTIVITY_SEC          30
# If you are using an access point, set PEER_TO_PEER to "N" for better
# performance.
        PEER_TO_PEER            N
#       FRAME                   ethernet_802.3
        FRAME                   ETHERNET_II
NetWare DOS Requester
        FIRST NETWORK DRIVE = G
        PREFERRED SERVER = ENTERPRISE
        NAME CONTEXT = "o = first_floor"
```

AUTOEXEC.BAT for NetWare

The following lines show some ODI driver files loaded from AUTOEXEC.BAT for a PEN*KEY 6100 Computer in a NetWare environment:

```
lsl.com
rl2oem.com
ipxodi
vlm
```

AUTOEXEC.BAT for TCP/IP

The following lines show some ODI driver files loaded from AUTOEXEC.BAT for a PEN*KEY 6100 Computer in a TCP/IP environment:

```
lsl.com
rl2oem.com
odipkt.com (this is the ODI to packet driver shim provided by FTP
Software)
ethdrv (or vxdinit for Windows enhanced mode only)
set pctcp = c:\ftp\pctcp.ini
```

Additional lines would include the path statement for the FTP directory and the SET command for PC/TCP.

NDIS Driver for TCP/IP

The NDIS driver for the PEN*KEY 6100 Computer is RL2OEM.DOS. The driver uses the parameters in the PROTOCOL.INI file, plus PROTMAN.EXE, PROTMAN.DOS, and NETBIND.COM.

PROTOCOL.INI

Following is an example of a PROTOCOL.INI file.

```
[protman]
DriverName = PROTMAN$

[RL2OEM]
drivername = RL2OEM$
;
; The 2.4 GHz radio in the PEN*KEY 6100 Computer uses IRQ 15.
;
INT = 15
;
; The 2.4 GHz radio in the PEN*KEY 6100 Computer uses 0x3f0.
;
PORT = 0x3f0
;
; Valid channel values are 1–15
;
; CHANNEL = 7
;
; Valid sub-channel values are 1–15
;
```

```
;SUBCHANNEL = 7
;
; Valid domain values are 0–15
;
DOMAIN = 7
;
; Valid station_type values are 0, 1, & 2
;
STATION_TYPE = 0
;
; Valid roam_config values are 0, 1, & 2
;
ROAM_CONFIG = 1
;
Valid mac_optimize values are 0 & 1
;
MAC_OPTIMIZE = 1
;
; Valid peer_to_peer values are Y & N
;
PEER_TO_PEER = N
INACTIVITY_MIN = 0
INACTIVITY_SEC = 0

[PKTDRV]
DriverName = PKTDRV$
intvec = 0x60
chainvec = 0 x 62
BINDINGS = RL2OEM
```

CONFIG.SYS

The following lines show some NDIS driver files loaded from CONFIG.SYS for a PEN*KEY 6100 Computer in a TCP/IP environment:

`device = a:\proxim\protman.dos /I:a:\proxim` *(/I specifies the path to `protocol.ini`)*
`device = a:\proxim\rl2oem.dos`
`device = a:\proxim\dis_pkt.gup` *(this is the NDIS to packet driver shim provided by FTP Software)*

Open Wireless LAN Parameters

The following ODI and NDIS parameters affect the PEN*KEY 6100 Computer's performance on the open wireless LAN.

CHANNEL and SUBCHANNEL

CHANNEL sets the hopping sequence of the radio. SUBCHANNEL differentiates between subnetworks These two parameters apply if the PEN*KEY 6100 Computer is an Alternate Master in a peer-to-peer (ad hoc) network. See STATION_TYPE on the next page for a description of Alternate Master.

DOMAIN

The value for DOMAIN must match the LAN ID specified for the 6710 Access Point.

FRAME

FRAME applies to the ODI driver only. Its value must match the frame type of the Ethernet host. Common values are "ETHERNET_II" (DIX Ethernet) and "ETHERNET_802.3."

INACTIVITY_MIN and INACTIVITY_SEC

These parameters set the snooze mode timeout for the Proxim 2.4 GHz radio option. When the radio is in snooze mode, it does not reliably hear broadcast or multicast messages. If the application depends on the PEN*KEY 6100 Computer hearing broadcast or multicast messages when the radio might be snoozing, these parameters must be disabled (set to "0"). Note that these parameters are not related to the computer's power management timeout parameters.

MAC_OPTIMIZE

The value for MAC_OPTIMIZE should be "0" when 20 or fewer PEN*KEY 6100 Computers are communicating with a 6710 Access Point. MAC_OPTIMIZE should be "1" for 21 or more computers. The parameter should be "1" even if 21 or more computers will be communicating with one access point for a short time.

▶ NOTE: *The best value depends on the site's particular operating environment. A Norand Systems Engineer should determine the appropriate value.*

PEER-TO-PEER

If the network is in a peer-to-peer (ad hoc) configuration, the value for this parameter must be "Y." If the PEN*KEY 6100 Computer is communicating through a 6710 Access Point, the value should be "N" for best performance. For most installations, the value will be "N."

ROAM_CONFIG

ROAM_CONFIG determines how the PEN*KEY 6100 Computer uses its internal RSSI values. The value for ROAM_CONFIG should be as follows:

- "0" if the computer will infrequently roam from one AP to another. The computer tries to stay with one access point longer.
- "1" if the access points' coverage areas overlap by some degree.
- "2" when the coverage areas of several access points have a large amount of overlap. The computer would quickly switch to the access point with the best RSSI levels.

▶ NOTE: *The best value depends on the site's particular operating environment. A Norand Systems Engineer should determine the appropriate value.*

STATION_TYPE (Ad Hoc)

The Proxim 2.4 GHz radio option has a mechanism where one Master station coordinates communications among other stations. All stations refer to the Master to determine where and when to hop. If a Master is not present, a station configured as an Alternate Master becomes the Master for a session. If a Master is present, the Alternate Master acts as a Station. Alternate Masters and Masters are usually found in peer-to-peer (ad hoc) networks, which do not contain 6710 Access Points.

Most open wireless LANs contain access points. In almost all cases, the access point is the Master and the PEN*KEY 6100 Computer is a Station. Therefore, STATION_TYPE should be "0" (Station) for the PEN*KEY 6100 Computer in a client-server–based network.

A peer-to-peer network leaves you with the task of configuring each PC-compatible computer on the open wireless LAN as Master, Alternate Master, or Station. In most cases, using the default values for each driver will work. However, you may need to change the configuration for performance or other issues. Following are some factors to consider for a peer-to-peer network:

- At most, one station must act as Master. If additional Masters will be set up, you should configure them as Alternate Masters so only one Master is on the network.
- The Master must be within radio range of the PC-compatible computers.
- The Master should be a station that will be stationary or remain on.
- Best performance results from configuring the fewest number of PC-compatible computers as Masters or Alternate Master.

Appendix D

6710 Access Point Specifications

About This Appendix

This appendix contains product, electrical, and environmental specifications for the 6710 Access Point. This appendix also describes the functionality of the access point's DIAG port.

Product Specifications

Following are product specifications for the access point.

Processor:	AMD 29200 RISC
Memory:	4 MB RAM/2 MB FLASH ROM
Distribution LAN compatibility:	ANSI/IEEE 802.3 (Ethernet communication standard) and DIX Version 2.0
Interface:	10BASE2 (thinnet), 10BASE5 (AUI or thicknet), and 10BASE-T (twisted pair) through ports on bottom panel
Card slots:	Two PC card-compatible slots
Mounting options:	Tabletop, wall, or ceiling

Electrical Specifications

The access point has one IEC connector for industry-standard three conductor ac input. The access point's internal power supply automatically detects the voltage level and frequency of the source power. Following are source power specifications.

Voltages:	Autosensing 110, 220, and 240 V ac
Frequency:	50 to 60 Hz
Safety:	UL/CSA (Underwriters Laboratory/ Canadian Standards Association), United States and Canada; CB (Competent Body) report for Europe

The access point complies with the following standards.

Immunity:	EN (Euro Norm) 50082-1 Generic Immunity Standard and ETS (European Telecommunication Standard) 300–339 Radio Equipment and Systems; Generic EMC (Electromagnetic Compatibility) for Radio Equipment
Emissions:	FCC Class B verified and CISPR* 22 (EN 55022) Class B radiated and conducted emissions under EN 50081-1, Generic Emissions Standard

* Comite International Special des Perturpations Radioelecturques/ International Special Committee on Radio Interference

Environmental Specifications

Following are environmental specifications for the access point.

Approximate size:	14.25 in x 6.80 in x 3.50 in (LWH) (36.19 cm x 17.27 cm x 8.89 cm)
Approximate weight:	3.75 lbs (1.70 kg)
Operating temperature (standard):	–4 °F to 122 °F (–20 °C to 50 °C)
Operating temperature (in NEMA enclosure):	–22 °F to 122 °F (–30 °C to 50 °C)
Humidity:	Up to 90 percent noncondensing

DIAG Port

The DIAG port is a 9-pin serial channel which provides access to the ROM command monitor and FLASH command interpreter. The port also provides the ability to reprogram FLASH, run manufacturing diagnostics, and view and set EEPROM parameters.

Appendix E

Host Connectivity Device Specifications

About This Appendix

This appendix contains product, electrical, and environmental specifications for the RC4030E Gateway and 6950 Enterprise Gateway Server. This appendix also describes the functionality of the RC4030E Gateway's DIAG and HOST ports.

RC4030E Gateway

Product Specifications

Following are product specifications for the RC4030E Gateway.

Processor:	Motorola 68302
Memory:	2 MB RAM/512 KB FLASH
Compatibility:	ANSI/IEEE 802.3 (Ethernet communication standard) and DIX Ethernet
Interface:	10BASE2 (thinnet) through BNC port; 10BASE-T (UTP) through UTP port
Mounting options:	Tabletop or wall

Electrical Specifications

Following are source power specifications for the United States and Canada.

Input voltage:	120 V ac
Output voltages:	+9.0 V dc, +13.5 V dc
Frequency:	60 Hz
Power consumption:	30 watts
Safety:	UL/CSA (Underwriters Laboratory/Canadian Standards Association), United States and Canada; CB (Competent Body) report for Europe

A different power supply is available for Europe and other areas having 230 V ac, 50 Hz power with TUV (Technischer Uberwachungs Verien/ Technical Supervision Society) approval. Another type of power supply is available for Japan and other areas having 100 V ac, 50 or 60 Hz power with MITI approval. Contact your Norand representative for more information about power supplies for international markets.

The RC4030E Gateway complies with the following standards.

Immunity:	EN (Euro Norm) 50082-1 Generic Immunity Standard
Emissions:	FCC Class B verified and CISPR* 22 (EN 55022) Class B radiated and conducted emissions under EN 50081-1, Generic Emissions Standard

* Comite International Special des Perturpations Radioelecturques/ International Special Committee on Radio Interference)

Environmental Specifications

Following are environmental specifications for the RC4030E Gateway.

Approximate size:	12.0 in x 6.4 in x 2.5 in (LWH) (30.48 cm x 16.26 cm x 6.35 cm)
Approximate weight:	4.30 lbs (1.95 kg)
Operating temperature:	–22 to 122 °F (–30 to 50 °C)
Humidity:	5 to 95 percent noncondensing

DIAG Port

The RC4030E Gateway's DIAG port is the channel through which gateway management tasks are done. Tasks include configuring and upgrading the gateway's system software, and checking the gateway's current FLASH and ROM versions. Following are DIAG port parameters.

Connector:	9-pin, D-subminiature female
Clocking:	Asynchronous
Type:	DTE
Interface:	RS-232

HOST Port

The RC4030E Gateway connects to the host computer through the gateway's HOST port. Following are HOST port parameters.

Connector:	25-pin, D-subminiature female
Clocking:	Asynchronous or synchronous
Type:	DTE
Interface:	RS-232 or V.35
Baud rate:	Asynchronous: 300 to 57600 bps Synchronous RS-232 and V.35: 1200 to 64000 bps, and external

6950 Enterprise Gateway Server

Product Specifications

Following are product specifications for the 6950 Enterprise Gateway Server.

Compatibility:	ANSI/IEEE 802.3 (Ethernet communication standard) and DIX Ethernet
Interface:	10BASE2 (thinnet), 10BASE5 (AUI or thicknet), and 10BASE-T (twisted pair) through installed Ethernet network interface card
Card slots:	5-slot back-plane
Mounting options:	Tabletop or wall

Electrical Specifications

The 6950 Enterprise Gateway Server's internal power supply autodetects the voltage level and frequency of the source power. The following chart lists source power specifications.

Input voltages:	Autosensing 110, 220, and 240 V ac
Output voltages:	+5.0 V ac and +12.0 V dc
Frequency:	50 to 60 Hz
Power consumption:	65 watts
Safety:	UL/CSA, United States and Canada; CB report for Europe

The 6950 Enterprise Gateway Server complies with the following standards.

Immunity:	EN 50082-1 Generic Immunity Standard
Emissions:	FCC Class B verified and CISPR 22 (EN 55022) Class B radiated and conducted emissions under EN 50081-1, Generic Emissions Standard

Environmental Specifications

Following are environmental specifications for the 6950 Enterprise Gateway Server.

Approximate size:	16.87 in (17.86 in with handle) x 4.32 in x 8.72 in (LWH) (42.85 cm, 45.36 cm with handle, x 10.97 cm x 22.15 cm)
Approximate weight:	12.00 lbs (5.44 kg)
Operating temperature:	32 to 140 °F (0 to 60 °C)
Humidity:	0 to 95 percent noncondensing